Math-Net.Ru

Общероссийский математический портал

А. В. Иванов, Незамкнутость класса гипер-бент-функций относительно действия полной линейной группы, *Матем. вопр. криптогр.*, 2012, том 3, выпуск 2, 5–26

DOI: <https://doi.org/10.4213/mvk52>

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: 52.23.180.231

26 апреля 2023 г., 14:17:28

УДК 579.716.32

Незамкнутость класса гипер-бент-функций относительно действия полной линейной группы

А. В. Иванов

Московский государственный технический университет радиотехники,
электроники и автоматики, г. Москва

Получено 20.V.2011

Рассматривается представление булевых функций отображениями из расширения конечного поля в его простое подполе. Исследуется влияние на свойства гипер-бент-функции действия на ее аргумент преобразований из полной линейной группы. Показано, что класс гипер-бент-функций не замкнут относительно действия таких преобразований.

Ключевые слова: бент-функция, гипер-бент-функция, мономиальная функция, полная линейная группа

Noncloseness of hyper-bent-function class under the general linear group action

A. V. Ivanov

*Moscow State Technical University of Radio Engineering, Electronics and Automatics,
Moscow*

Abstract. Representations of Boolean functions by mappings of finite field extension to its simple subfield are considered. The effect of transforming the argument of hyper-bent-function by general linear group on properties of this function is studied. It is shown that the class of hyper-bent-functions is not closed under such transforms.

Key words: bent-function, hyper-bent-functions, monomial function, general linear group

Citation: *Mathematical Aspects of Cryptography*, 2012, vol. 3, no. 2, pp. 5–26 (Russian).

Работа выполнена при поддержке гранта Президента РФ НШ-8.2010.10

© 2012 А. В. Иванов

Пусть $\mathbb{F}_2 = \text{GF}(2)$ — поле из двух элементов, e — единица поля $\mathbb{F}_2$, $\mathbb{F}_{2^n} = \text{GF}(2^n)$ — расширение поля $\mathbb{F}_2$ натуральной степени n , $\text{tr}_t^n(\alpha) = \sum_{k=0}^{(n/t)-1} \alpha^{2^{t \cdot k}}$ — функция след из поля $\mathbb{F}_{2^n}$ в его подполе $\mathbb{F}_{2^t} = \text{GF}(2^t)$ для каждого натурального t такого, что $t|n$. Для целого t через $\rho_n(t)$ будем обозначать число из множества $\{1, \dots, 2^n - 1\}$, определяемое условием $\rho_n(t) \equiv t \pmod{2^n - 1}$. Для целых чисел t_1, t_2 через (t_1, t_2) будем обозначать их неотрицательный наибольший общий делитель. Через $\mathcal{B}_n$ обозначим множество булевых функций от n переменных, через $\mathcal{F}_n$ — множество всех отображений поля $\mathbb{F}_{2^n}$ в поле $\mathbb{F}_2$.

В работе изучаются свойства класса гипер-бент-функций (см. [1, 2, 4, 9, 18]), являющегося подмножеством множества $\mathcal{F}_n$. С учетом взаимно однозначного соответствия множеств $\mathcal{B}_n$ и $\mathcal{F}_n$ при фиксированном базисе векторного пространства $(\mathbb{F}_{2^n})_{\mathbb{F}_2}$ рассмотрены вопросы, связанные с действием полной линейной группы на множестве гипер-бент-функций. Известно, что множество бент-функций замкнуто относительно действия преобразований из полной линейной группы на аргумент функции. В этом отношении полученные результаты демонстрируют отличие свойств класса гипер-бент-функций от класса бент-функций.

§ 1. Представление булевых функций отображениями из множества $\mathcal{F}_n$

Рассмотрим произвольную функцию φ из множества $\mathcal{B}_n$. Зафиксируем базис

$$(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1}) \quad (1)$$

поля $\mathbb{F}_{2^n}$ как векторного пространства над полем $\mathbb{F}_2$. Для любого набора булевых величин $x_0, x_1, \dots, x_{n-1}$ однозначно определен элемент x поля $\mathbb{F}_{2^n}$:

$$x = \sum_{j=0}^{n-1} x_j \cdot \varepsilon_j. \quad (2)$$

Сопоставив согласно соотношению (2) каждому набору значений n аргументов функции φ элемент поля $\mathbb{F}_{2^n}$, зададим значения отображения

$F \in \mathcal{F}_n$ для каждого $x = \sum_{j=0}^{n-1} x_j \cdot \varepsilon_j \in (\mathbb{F}_2)^n$ равенством

$$F\left(\sum_{j=0}^{n-1} x_j \cdot \varepsilon_j\right) = \varphi(x_0, \dots, x_{n-1}). \quad (3)$$

Таким образом, определено взаимно однозначное соответствие между множествами $\mathcal{B}_n$ и $\mathcal{F}_n$. Функцию $\varphi \in \mathcal{B}_n$ и отображение $F \in \mathcal{F}_n$, связанные равенством (3), будем называть *соответствующими в базисе* $(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1})$.

В [1] показано, что отображение F можно представить многочленом вида

$$F(x) = \text{tr}_1^n(\Phi(x)) + c_0, \quad (4)$$

где $c_0 \in \mathbb{F}_2$, а $\Phi(x)$ — некоторый полином над полем $\mathbb{F}_{2^n}$ со свойством $\Phi(0) = 0$, который, вообще говоря, определен неоднозначно (это связано с понятием *эквивалентности полиномов по следу*, см. [3]). Для получения однозначного представления вводят ряд дополнительных условий (см., например, [1]).

Через M_n обозначим набор минимальных представителей всех различных *циклотомических классов* (см., например, монографию [5]) множества чисел $\{1, \dots, 2^n - 1\}$. Через $C_{n,t}$ обозначим циклотомический класс с представителем t . Если t — наименьшее число в классе (т. е. $t \in M_n$), то

$$C_{n,t} = \{t, \rho_n(t \cdot 2), \rho_n(t \cdot 2^2), \dots, \rho_n(t \cdot 2^{r_{n,t}-1})\},$$

где значение $r_{n,t}$ (мощность класса $C_{n,t}$) определяется условием

$$r_{n,t} = \min\{k \in \mathbb{N}_0 \mid t \cdot 2^k \equiv t \pmod{2^n - 1}\}. \quad (5)$$

Заметим, что $r_{n,t} \mid n$ и $r_{n,t} = n$, если $(t, 2^n - 1) = 1$.

Выберем и зафиксируем систему элементов

$$\Xi_n = \{\xi_{n,t} \in \mathbb{F}_{2^n} \mid \text{tr}_{r_{n,t}}^n(\xi_{n,t}) = e, t \in M_n\}. \quad (6)$$

В [1] показано, что многочлен $\Phi(x)$ в равенстве (4) может быть выбран в виде

$$\Phi(x) = \sum_{t \in M_n} c_t \cdot \xi_{n,t} \cdot x^t, \quad (7)$$

где $c_t \in \mathbb{F}_{2^{n,t}}$ для каждого $t \in M_n$.

Многочлен $\Phi(x)$ вида (7) называют *редуцированным многочленом* (см. [1]), а представление (4), где многочлен $\Phi(x)$ имеет вид (7), — *приведенным представлением отображения F в системе Ξ_n* , а также *приведенным представлением булевой функции φ над полем $\mathbb{F}_{2^n}$ в системе Ξ_n и базисе $(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1})$* (см. [1]). Заметим, что вид приведенного представления булевой функции и свойства соответствующего ей отображения из множества $\mathcal{F}_n$ зависят от выбираемого базиса.

Индекс нелинейности ([1]) редуцированного многочлена $\Phi(x)$ вида (7) определяется равенством

$$\text{ind } \Phi(x) = \max \{ \|t\|_2 \mid t \in M_n, c_t \neq 0 \},$$

где через $\|t\|_2$ обозначен *двоичный вес* числа $t \in M_n$, т. е. количество ненулевых цифр в записи t в двоичной системе счисления. С учетом наших обозначений и определений приведем в следующей формулировке один из результатов работы [1].

Теорема 1. Пусть n — натуральное число, Ξ_n — фиксированная система элементов поля $\mathbb{F}_{2^n}$, определенная равенством (6), $(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1})$ — базис векторного пространства $(\mathbb{F}_{2^n})_{\mathbb{F}_2}$. Тогда для любой булевой функции $\varphi \in \mathcal{B}_n$ существует единственное приведенное представление над полем $\mathbb{F}_{2^n}$ в системе Ξ_n и базисе $(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1})$. При этом степень нелинейности функции φ равна индексу нелинейности редуцированного многочлена приведенного представления.

ЗАМЕЧАНИЕ 1. 1) Представление функций из множества $\mathcal{B}_n$ многочленами над полем $\mathbb{F}_{2^n}$, а также связь степени нелинейности булевой функции с максимальным из двоичных весов показателей степеней мономов многочлена, функция след от которого задает эту булеву функцию в некотором базисе пространства $(\mathbb{F}_{2^n})_{\mathbb{F}_2}$, использовались и другими авторами (см., напри-

мер, [3, 10, 16]). Однако здесь мы ссылаемся на статью [1], так как именно в ней введен термин «приведенное представление».

2) Везде далее для каждого натурального числа n система элементов Ξ_n считается фиксированной, и при употреблении термина «приведенное представление» слова «в системе Ξ_n » могут опускаться.

3) Из теоремы 1, в частности, следует, что индекс нелинейности редуцированного многочлена приведенного представления булевой функции в некотором базисе пространства $(\mathbb{F}_{2^n})_{\mathbb{F}_2}$ не зависит от выбора базиса. Таким образом, для любого числа $i \in \{1, \dots, n\}$ множество приведенных представлений всех булевых функций степени i также не зависит от выбора базиса пространства $(\mathbb{F}_{2^n})_{\mathbb{F}_2}$. Множества отображений из $\mathcal{F}_n$, соответствующих всем линейным и всем аффинным булевым функциям от n переменных, имеют вид

$$\mathcal{L}_n = \{ \text{tr}_1^n (c_1 \cdot x) \mid c_1 \in \mathbb{F}_{2^n} \}$$

и

$$\mathcal{A}_n = \{ \text{tr}_1^n (c_1 \cdot x) + c_0 \mid c_0 \in \mathbb{F}_2, c_1 \in \mathbb{F}_{2^n} \}$$

соответственно.

Условимся везде далее для элемента $\alpha \in \mathbb{F}_2$ под $(-1)^\alpha$ понимать целое число -1 , если $\alpha = e$, и целое число 1 , если $\alpha = 0$. Преобразованием Уолша–Адамара булевой функции $\varphi \in \mathcal{B}_n$ называют целочисленную функцию на множестве $(\mathbb{F}_2)^n$, значения которой определяются равенством

$$W_\varphi(c_0, \dots, c_{n-1}) = \sum_{(x_0, \dots, x_{n-1}) \in (\mathbb{F}_2)^n} (-1)^{\varphi(x_0, \dots, x_{n-1}) + c_0 x_0 + \dots + c_{n-1} x_{n-1}}. \quad (8)$$

Для каждого элемента $\vec{c} \in (\mathbb{F}_2)^n$ значение $W_\varphi(\vec{c})$ называют коэффициентом Уолша–Адамара функции φ .

Заметим, что из соображений удобства при решении конкретных задач здесь приведено определение коэффициента Уолша–Адамара в соответствии с монографиями [4] и [5]. Однако в ряде других работ, в том числе в монографии [7], термин «коэффициент Уолша–Адамара второго рода» используется для коэффициентов (8), нормированных множителем $1/2^n$.

Из равенства Парсеваля (см., например, [4, 5, 7]) следует, что для любой функции $\varphi \in \mathcal{B}_n$ выполняется условие

$$\max \left\{ \left| W_\varphi(\tilde{c}) \right| \mid \tilde{c} \in (\mathbb{F}_2)^n \right\} \geq 2^{\frac{n}{2}}. \quad (9)$$

Функции из множества $\mathcal{B}_n$, у которых все коэффициенты Уолша–Адамара по модулю равны $2^{n/2}$, называют *бент-функциями*. Булевы бент-функции существуют только для четных значений n (см., например, [11, 17]). В [17] показано, что все булевы бент-функции от n переменных, где n больше 2 и четно, имеют степень нелинейности не больше $n/2$.

При любом фиксированном базисе пространства $(\mathbb{F}_{2^n})_{\mathbb{F}_2}$, используя взаимно однозначное соответствие (3) множеств $\mathcal{F}_n$ и $\mathcal{B}_n$, для отображений из множества $\mathcal{F}_n$ можно естественным образом определить аналогичные известным для булевых функций понятия веса функции, расстояния между функциями, расстояния от функции до множества, нелинейности функции ([4]). В качестве характеристики близости функции $G \in \mathcal{F}_n$ к функции $F \in \mathcal{F}_n$ будем также использовать параметр $\Delta(F, G)$ (см. [1, 2]), определяемый равенством

$$\Delta(F, G) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{F(x)+G(x)}. \quad (10)$$

В случае когда функция G соответствует некоторой линейной булевой функции (т. е. $G \in \mathcal{L}_n$), параметр $\Delta(F, G)$ будем называть *коэффициентом Уолша–Адамара* функции F . Для таких коэффициентов мы будем использовать отдельное обозначение

$$\Delta_c^{(F)} = \Delta(F, \text{tr}_1^n(cx)), \text{ где } c \in \mathbb{F}_{2^n}. \quad (11)$$

ЗАМЕЧАНИЕ 2. Для соответствующих друг другу функции $\varphi \in \mathcal{B}_n$ и отображения $F \in \mathcal{F}_n$ перечисленные выше одноименные числовые характеристики одинаковы. Из этого, в частности, следует, что для любого отображения $F \in \mathcal{F}_n$ выполнено соотношение

$$\max \left\{ \left| \Delta_c^{(F)} \right| \mid c \in \mathbb{F}_{2^n} \right\} \geq 2^{\frac{n}{2}}. \quad (12)$$

Функции из множества $\mathcal{F}_n$, для которых все коэффициенты Уолша–Адамара по модулю равны $2^{n/2}$, будем называть *бент-функциями*. Если

функция $\varphi \in \mathcal{B}_n$ соответствует отображению $F \in \mathcal{F}_n$ в некотором базисе пространства $(\mathbb{F}_{2^n})_{\mathbb{F}_2}$, то φ является бент-функцией тогда и только тогда, когда F является бент-функцией. Таким образом, множество $\mathcal{F}_n$ содержит бент-функции, если и только если n четно. Из теоремы 1 следует, что если функция $F \in \mathcal{F}_n$ является бент-функцией, то индекс нелинейности редуцированного многочлена ее приведенного представления не превосходит $n/2$.

§ 2. Мономиальные функции и гипер-бент-функции

Функция из множества $\mathcal{F}_n$ принадлежит классу *мономиальных функций* ([1, 13, 18]), если она представима в виде

$$L_c^{(\delta)}(x) = \text{tr}_1^n(c \cdot \xi_{n,\delta} \cdot x^\delta), \quad \delta \in M_n, c \in \mathbb{F}_{2^{n,\delta}}.$$

Другими словами, функция входит в данный класс, если в ее приведенном представлении соответствующий редуцированный многочлен является мономом. Если показатель степени δ взаимно прост с числом $2^n - 1$, то функцию $L_c^{(\delta)}$ при любом $c \in \mathbb{F}_{2^{n,\delta}}$ будем, следуя работе [1], называть *собственной мономиальной*.

Заметим, что для любого $c \in \mathbb{F}_{2^n}$ отображение $L_c^{(1)}$ лежит в классе $\mathcal{L}_n$. Поэтому из оценки (12) следует, что для любой функции $F \in \mathcal{F}_n$

$$\max \left\{ \left| \Delta(F, L_c^{(\delta)}) \right| \mid \delta \in M_n, (\delta, 2^n - 1) = 1, c \in \mathbb{F}_{2^n} \right\} \geq 2^{n/2}. \quad (13)$$

Функции из множества $\mathcal{F}_n$, для которых оценка (13) обращается в равенство, принято называть *гипер-бент-функциями*. Впервые такое название для функций с данным свойством ввели А. Йозеф и Г. Гонг в [18]. В той же работе был построен пример класса гипер-бент-функций из множества $\mathcal{F}_n$ для любого четного $n > 2$, описанный в терминах линейных рекуррентных последовательностей. Позднее в работах [1, 9] для данного класса были предложены более удобные эквивалентные определения.

Теорема 2 ([9]). Пусть n — четное число, α — примитивный элемент поля $\mathbb{F}_{2^n}$ и для отображения $F \in \mathcal{F}_n$ выполнены условия

$$F(0) = 0, \quad F(\alpha^{2^{n/2}+1}x) = F(x) \quad \text{для всех } x \in \mathbb{F}_{2^n}.$$

Тогда F является гипер-бент-функцией, если и только если количество единиц в векторе $(F(e), F(\alpha), F(\alpha^2), \dots, F(\alpha^{2^{n/2}}))$ равно $2^{n/2-1}$.

Кроме того, в [9] было показано, что все гипер-бент-функции F из данного класса со свойством $F(e) = 0$ составляют известный класс бент-функций $\mathcal{PS}_{ap}$, описанный в 1974 году в работе [12]. А те гипер-бент-функции, для которых $F(e) = e$, представимы в виде $F(x) = F'(\beta x)$, где $F' \in \mathcal{PS}_{ap}$, $\beta \in \mathbb{F}_{2^n}^*$, $F'(\beta) = e$. В связи с этим было предложено обозначать весь класс гипер-бент-функций из множества $\mathcal{F}_n$, описываемых теоремой 2, расширенный за счет прибавления константы, через $\mathcal{PS}_{ap}^\#(n)$. Везде далее через $\mathcal{PS}_{ap}^{\#,0}(n)$ будем обозначать множество сохраняющих нуль отображений из класса $\mathcal{PS}_{ap}^\#(n)$ (т. е. $\mathcal{PS}_{ap}^{\#,0}(n) = \{F \in \mathcal{PS}_{ap}^\#(n) \mid F(0) = 0\}$).

ЗАМЕЧАНИЕ 3. Из определения гипер-бент-функции следует, что если функция $F \in \mathcal{F}_n$ является гипер-бент-функцией, то для любого числа $\delta \in \{1, \dots, 2^n - 1\}$, взаимно простого с $2^n - 1$, функция $F_\delta \in \mathcal{F}_n$, значения которой определяются для каждого $x \in \mathbb{F}_{2^n}$ равенством $F_\delta(x) = F(x^\delta)$, также является гипер-бент-функцией (см. [1]).

Из результатов работы [1] следует справедливость теоремы 3.

Теорема 3. Пусть $n > 2$ — четное число, $(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1})$ — базис векторного пространства $(\mathbb{F}_{2^n})_{\mathbb{F}_2}$, φ — булева функция от n переменных. Если редуцированный многочлен приведенного представления функции φ в базисе $(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1})$ содержит хотя бы один моном такой степени t , что существует число $t' \in \{1, \dots, 2^n - 2\}$, удовлетворяющее условиям

$$a) \quad (t', 2^n - 1) = 1,$$

$$b) \quad \|\rho_n(t \cdot t')\|_2 \neq \frac{n}{2},$$

то отображение из множества $\mathcal{F}_n$, соответствующее функции φ в базисе $(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1})$, не является гипер-бент-функцией.

ЗАМЕЧАНИЕ 4. Из теорем 1 и 3 следует, что степень нелинейности булевой функции от n переменных, соответствующей в некотором базисе гипер-бент-функции, равна $n/2$.

§ 3. Действие на функции из $\mathcal{PS}_{ap}^{\#,0}(n)$ преобразований из полной линейной группы на множестве их аргументов

Известно, что класс бент-функций является замкнутым относительно действия преобразований из полной линейной группы на аргумент функции. Также известно, что все булевы бент-функции от четырех переменных аффинно эквивалентны. Кроме того, проведена аффинная классификация булевых бент-функций от 6 (см. [17]) и 8 (см. [14, 15]) переменных (см. также подробный обзор в [8]). Полную аффинную классификацию булевых бент-функций от 10 переменных и более пока провести не удастся.

Так как булевы функции, соответствующие гипер-бент-функциям из множества $\mathcal{F}_n$, имеют степень нелинейности, равную $n/2$, нас интересуют классы линейной (аффинной) эквивалентности именно таких бент-функций.

Экспериментально установлено (см. работу [17]), что любая бент-функция степени 3 от 6 переменных эквивалентна с точностью до невырожденных аффинных замен переменных и добавления произвольных аффинных функций одной из следующих трех функций:

$$y_1 y_2 y_3 + y_1 y_4 + y_2 y_5 + y_3 y_6;$$

$$y_1 y_2 y_3 + y_2 y_4 y_5 + y_1 y_2 + y_1 y_4 + y_2 y_6 + y_3 y_5 + y_4 y_5$$

или

$$y_1 y_2 y_3 + y_2 y_4 y_5 + y_3 y_4 y_6 + y_1 y_4 + y_2 y_6 + y_3 y_4 + y_3 y_5 + y_3 y_6 + y_4 y_5 + y_4 y_6. \quad (14)$$

В процессе подготовки настоящей работы автором совместно с М. К. Датиным было проведено экспериментальное исследование того, как действует на множестве сохраняющих нуль гипер-бент-функций из $\mathcal{F}_6$ (согласно [1], оно совпадает с классом $\mathcal{PS}_{ap}^{\#,0}(6)$) полная линейная группа на множестве их аргументов. Было установлено, что все сохраняющие нуль гипер-бент-функции из множества $\mathcal{F}_6$ соответствуют булевым бент-функциям от 6 переменных из класса с представителем (14). Кроме того, оказалось, что для любой пары сохраняющих нуль гипер-бент-функций из множества $\mathcal{F}_6$ существует обратимое линейное преобразование, переводящее одну функцию в другую.

Подобный эксперимент для больших значений n на современных вычислительных средствах трудно осуществим за приемлемое время. Однако некоторые свойства могут быть доказаны в общем случае.

Зафиксируем базис

$$(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1}) \quad (15)$$

поля $\mathbb{F}_{2^n}$ как векторного пространства над полем $\mathbb{F}_2$. Пусть отображение T ставит в соответствие каждому элементу множества $\mathbb{F}_{2^n} \setminus \{0\}$ строку координат разложения этого элемента по базису (15). Тем самым отображение T задает биективное соответствие между множествами $\mathbb{F}_{2^n} \setminus \{0\}$ и $(\mathbb{F}_2)^n \setminus \{\bar{0}\}$. Через χ обозначим индуцируемый отображением T изоморфизм симметрических групп подстановок $S(\mathbb{F}_{2^n} \setminus \{0\})$ и $S((\mathbb{F}_2)^n \setminus \{\bar{0}\})$. Далее будем рассматривать полную линейную группу $GL(n, 2)$ как группу подстановок на множестве $(\mathbb{F}_2)^n \setminus \{\bar{0}\}$.

Утверждение 1. Для любого четного числа $n > 2$ класс $\mathcal{PS}_{ap}^{\#,0}(n)$ не замкнут относительно действия преобразований из полной линейной группы на аргумент функции.

Доказательство. Зафиксируем четное $n > 2$. Пусть $n = 2\lambda$. Согласно теореме 2, любое отображение $F \in \mathcal{F}_n$, лежащее в классе $\mathcal{PS}_{ap}^{\#,0}(n)$, обладает следующими свойствами:

$$1) F(0) = 0;$$

$$2) \text{ для некоторого примитивного элемента } \alpha \text{ поля } \mathbb{F}_{2^n} \text{ равенство } F(\alpha^{2^{\lambda}+1}x) = F(x) \text{ выполнено для всех } x \in \mathbb{F}_{2^n}.$$

Заметим, что для любого примитивного элемента α поля $\mathbb{F}_{2^n}$ множество $\left\{ \alpha^{2^{\lambda}+1}, (\alpha^{2^{\lambda}+1})^2, \dots, (\alpha^{2^{\lambda}+1})^{2^{\lambda}-1} \right\}$ совпадает с мультипликативной группой поля $\mathbb{F}_{2^{\lambda}} \subset \mathbb{F}_{2^n}$. Таким образом, условие 2) равносильно следующему:

$$2') \text{ для любого элемента } \beta \in \mathbb{F}_{2^{\lambda}}^* \subset \mathbb{F}_{2^n} \text{ равенство } F(\beta x) = F(x) \text{ выполнено для всех } x \in \mathbb{F}_{2^n}.$$

Зафиксируем $\beta \in \mathbb{F}_{2^n}^* \setminus \{e\}$. Пусть γ_0 и γ_1 — такие ненулевые элементы поля $\mathbb{F}_{2^n}$, что

$$F(\gamma_0) = 0, \quad (16)$$

$$F(\gamma_1) = e. \quad (17)$$

Выберем ненулевой элемент $\gamma \in \mathbb{F}_{2^n}$. Заметим, что γ и $\gamma \cdot \beta$ как элементы векторного пространства $(\mathbb{F}_{2^n})_{\mathbb{F}_2}$ линейно независимы. В том же смысле линейно независимыми являются γ_0 и γ_1 . Тогда существует такое обратимое линейное преобразование L векторного пространства $(\mathbb{F}_{2^n})_{\mathbb{F}_2}$, что

$$L(\gamma) = \gamma_0, \quad (18)$$

$$L(\gamma \cdot \beta) = \gamma_1. \quad (19)$$

Рассмотрим отображение $G \in \mathcal{F}_n$, определяемое для любого $x \in \mathbb{F}_{2^n}$ следующим образом

$$G(x) = F(L(x)).$$

В силу соотношений (16), (17), (18), (19) справедливо неравенство

$$G(\gamma) \neq G(\gamma \cdot \beta).$$

Таким образом, для отображения G не выполнено условие 2') и, следовательно, G не принадлежит классу $\mathcal{PS}_{ap}^{\#,0}(n)$. Утверждение доказано.

Утверждение 2. Пусть n — четное число, большее 16. Тогда множество $\mathcal{PS}_{ap}^{\#,0}(n)$ не содержится ни в одном классе линейной эквивалентности отображений из множества $\mathcal{F}_n$.

Доказательство. Предположим, что утверждение неверно. Тогда все гипер-бент-функции из класса $\mathcal{PS}_{ap}^{\#,0}(n)$ являются линейно эквивалентными. Следовательно, для фиксированного отображения $F \in \mathcal{PS}_{ap}^{\#,0}(n)$ и любого другого отображения $G \in \mathcal{PS}_{ap}^{\#,0}(n)$ существует такое обратимое линейное преобразование L_G векторного пространства $(\mathbb{F}_{2^n})_{\mathbb{F}_2}$, что для любого элемента x поля $\mathbb{F}_{2^n}$ выполнено равенство

$$F(L_G(x)) = G(x).$$

Заметим, что для выполнения этого условия необходимо, чтобы порядок группы $\chi^{-1}(\text{GL}(n, 2))$ был не меньше мощности множества $\mathcal{PS}_{ap}^{\#,0}(n)$, т. е. должно выполняться неравенство

$$|\chi^{-1}(\text{GL}(n, 2))| \geq |\mathcal{PS}_{ap}^{\#,0}(n)|. \quad (20)$$

Положим $\lambda = n / 2$. В [9, 18] показано, что

$$|\mathcal{PS}_{ap}^{\#,0}(n)| = C_{2^\lambda+1}^{2^{\lambda-1}}. \quad (21)$$

С другой стороны, известно, что

$$|\chi^{-1}(\text{GL}(n, 2))| = \prod_{i=0}^{n-1} (2^n - 2^i). \quad (22)$$

Для четных $n = 2, 4, \dots, 18$ значения выражений (21) и (22) были вычислены. При этом оказалось, что неравенство (20) не выполнено только в случае $n = 18$.

Оценим порядок роста величин $|\chi^{-1}(\text{GL}(n, 2))|$ и $|\mathcal{PS}_{ap}^{\#,0}(n)|$ по n . Из равенства (22) следует, что

$$\frac{|\chi^{-1}(\text{GL}(n+2, 2))|}{|\chi^{-1}(\text{GL}(n, 2))|} = \frac{\prod_{i=0}^{n+1} (2^{n+2} - 2^i)}{\prod_{i=0}^{n-1} (2^n - 2^i)} = \frac{\left(\prod_{i=2}^{n+1} 2^2 (2^n - 2^{i-2}) \right) (2^{n+2} - 2)(2^{n+2} - 1)}{\prod_{i=0}^{n-1} (2^n - 2^i)}.$$

Отсюда получим соотношение

$$\frac{|\chi^{-1}(\text{GL}(n+2, 2))|}{|\chi^{-1}(\text{GL}(n, 2))|} = 2^{2n} (2^{n+2} - 2)(2^{n+2} - 1). \quad (23)$$

Из равенства (21) следует, что

$$\begin{aligned} \frac{|\mathcal{PS}_{ap}^{\#,0}(2\lambda+2)|}{|\mathcal{PS}_{ap}^{\#,0}(2\lambda)|} &= \frac{C_{2^{\lambda+1}+1}^{2^\lambda}}{C_{2^\lambda+1}^{2^{\lambda-1}}} = \frac{(2^{\lambda+1}+1) \cdot (2^{\lambda+1})!}{(2^\lambda)! \cdot (2^{\lambda+1}+1-2^\lambda)!} \cdot \frac{(2^{\lambda-1})! \cdot (2^\lambda+1-2^{\lambda-1})!}{(2^\lambda+1) \cdot (2^\lambda)!} = \\ &= \frac{(2^{\lambda+1}+1) \cdot (2^{\lambda-1}+1)}{(2^\lambda+1) \cdot (2^\lambda+1)} \cdot \frac{(2^{\lambda+1})!}{(2^\lambda)!} \cdot \frac{(2^{\lambda-1})! \cdot (2^{\lambda-1})!}{(2^\lambda)! \cdot (2^\lambda)!} = \\ &= \frac{(2^{\lambda+1}+1) \cdot (2^{\lambda-1}+1)}{(2^\lambda+1) \cdot (2^\lambda+1)} \cdot \prod_{i=0}^{2^\lambda-1} (2^{\lambda+1}-i) \cdot \frac{1}{\left(\prod_{i=0}^{2^{\lambda-1}-1} (2^\lambda-i) \right)^2}. \end{aligned}$$

Таким образом,

$$\frac{|\mathcal{PS}_{ap}^{\#0}(2\lambda+2)|}{|\mathcal{PS}_{ap}^{\#0}(2\lambda)|} = \frac{(2^{\lambda+1}+1) \cdot (2^{\lambda-1}+1)}{(2^\lambda+1) \cdot (2^\lambda+1)} \cdot \prod_{i=0}^{2^{\lambda-1}-1} \frac{(2^{\lambda+1}-2i)(2^{\lambda+1}-2i-1)}{(2^\lambda-i)^2}. \quad (24)$$

Заметим, что

$$\frac{(2^{\lambda+1}+1) \cdot (2^{\lambda-1}+1)}{(2^\lambda+1) \cdot (2^\lambda+1)} = \frac{2^{2\lambda} + 5 \cdot 2^{\lambda-1} + 1}{2^{2\lambda} + 4 \cdot 2^{\lambda-1} + 1} > 1. \quad (25)$$

Кроме того, для любого $i \in \{0, \dots, 2^{\lambda-1}-1\}$ справедливы соотношения

$$\frac{(2^{\lambda+1}-2i)(2^{\lambda+1}-2i-1)}{(2^\lambda-i)^2} = 2 \left(2 - \frac{1}{2^\lambda-i} \right) > 2. \quad (26)$$

Из (24), (25) и (26) следует неравенство

$$\frac{|\mathcal{PS}_{ap}^{\#0}(2\lambda+2)|}{|\mathcal{PS}_{ap}^{\#0}(2\lambda)|} > 2^{2^{\lambda-1}}. \quad (27)$$

Сравнивая (27) и (23), находим, что при $\lambda \geq 7$ выполнено неравенство

$$\frac{|\mathcal{PS}_{ap}^{\#0}(2\lambda+2)|}{|\mathcal{PS}_{ap}^{\#0}(2\lambda)|} > \frac{|\chi^{-1}(\text{GL}(n+2, 2))|}{|\chi^{-1}(\text{GL}(n, 2))|}.$$

Из последнего неравенства и того, что $|\chi^{-1}(\text{GL}(18, 2))| < |\mathcal{PS}_{ap}^{\#}(18)|$, получим противоречие с неравенством (20). Утверждение доказано.

§ 4. Незамкнутость множества всех гипер-бент-функций относительно действия на их аргумент преобразований из полной линейной группы

Из результатов работ [1, 9, 18] следует, что для ряда четных значений числа n множество гипер-бент-функций из $\mathcal{F}_n$ совпадает с классом $\mathcal{PS}_{ap}^{\#}(n)$.

В этом случае из утверждения 1 следует незамкнутость множества всех сохраняющих нуль гипер-бент-функций относительно действия преобразований из полной линейной группы на аргумент функции. Доказательство этого

свойства для произвольного четного n использует ряд вспомогательных результатов.

Для всех чисел $d \in \{1, \dots, 2^n - 2\}$ через π_d будем обозначать преобразование множества $\mathbb{F}_{2^n} \setminus \{0\}$, определяемое для любого элемента $x \in \mathbb{F}_{2^n}$ равенством

$$\pi_d(x) = x^d. \quad (28)$$

Для различных чисел $d', d'' \in \{1, \dots, 2^n - 2\}$, каждое из которых взаимно просто с $2^n - 1$, отображения $\pi_{d'}$ и $\pi_{d''}$ задают различные подстановки на множестве $\mathbb{F}_{2^n} \setminus \{0\}$. Кроме того, для любых чисел $d', d'' \in \{1, \dots, 2^n - 2\}$ выполнено равенство

$$\pi_{d''} \circ \pi_{d'} = \pi_{d'd'' \bmod (2^n - 1)},$$

где « $\circ$ » — операция композиции отображений. Положим

$$\mathcal{D}_n = \left\{ \pi_d \mid d \in \{1, \dots, 2^n - 2\}, (d, 2^n - 1) = 1 \right\}$$

и заметим, что это множество с операцией композиции является абелевой группой.

Лемма 1. Для любого натурального числа $n > 4$ существует такое число $d \in \{1, \dots, 2^n - 2\}$, что $(d, 2^n - 1) = 1$, подстановка π_d нечетна, а подстановка $(\pi_d)^2$ не принадлежит множеству $\chi^{-1}(\text{GL}(n, 2))$.

Доказательство. Рассмотрим произвольное натуральное число $n > 4$. Известно (см., например, [5]), что все подстановки из множества $\chi^{-1}(\text{GL}(n, 2)) \cap \mathcal{D}_n$ имеют вид π_{2^t} , где $t \in \{0, \dots, n-1\}$. Подстановка $\pi_{2^{n-2}}$ нечетна, так как раскладывается в произведение $2^{n-1} - 1$ транспозиций. Следовательно, четность любой подстановки отличается от четности композиции этой подстановки с подстановкой $\pi_{2^{n-2}}$.

Таким образом, если существует такое число $d' \in \{1, \dots, 2^n - 2\}$, что

$$\pi_{(d')^2 \bmod (2^n - 1)} \in \mathcal{D}_n \setminus \left\{ \pi_{2^t} \mid t \in \{0, \dots, n-1\} \right\}, \quad (29)$$

то либо подстановка $\pi_{d'}$, либо подстановка $\pi_{2^n-1-d'}$ удовлетворяет условию леммы. Выполнение для числа d' условия (29) равносильно тому, что d' взаимно просто с 2^n-1 и двоичный вес числа $(d')^2$, взятого по модулю 2^n-1 , больше 1. Покажем существование таких d' . Пусть $n=2^{n_1}n_2$, где $(n_2, 2)=1$. Рассмотрим отдельно два случая.

1) Пусть $n_2 > 1$. Рассмотрим число $2^{2^{n_1}}+1$. С учетом того, что $(2^t-1, 2^t+1)=1$ для любого натурального числа t и

$$(2^{t_1}-1, 2^{t_2}-1)=2^{(t_1, t_2)}-1 \text{ для любых натуральных } t_1, t_2, \quad (30)$$

из свойств наибольшего общего делителя целых чисел следует справедливость равенств

$$(2^{2^{n_1}}+1, 2^n-1) = \frac{(2^{2^{n_1+1}}-1, 2^n-1)}{(2^{2^{n_1}}-1, 2^n-1)} = \frac{2^{(2^{n_1+1}, 2^{n_1}n_2)}-1}{2^{(2^{n_1}, 2^{n_1}n_2)}-1} = \frac{2^{2^{n_1}}-1}{2^{2^{n_1}}-1} = 1. \quad (31)$$

Так как $(2^{2^{n_1}}+1)^2 = 2^{2^{n_1} \cdot 2} + 2^{2^{n_1}+1} + 1$, то двоичный вес остатка от деления числа $(2^{2^{n_1}}+1)^2$ на 2^n-1 при $n_1=0$ равен 2, а при $n_1 > 0$ равен 3. В обоих случаях с учетом равенств (31) получим, что при $n_2 > 1$ в качестве d' можно выбрать число $2^{2^{n_1}}+1$.

2) Пусть теперь $n_2 = 1$. Заметим, что так как $n > 4$, а $n_2 = 1$, то

$$n_1 > 2. \quad (32)$$

Рассмотрим число $3 \cdot 2^{2^{n_1-1}-1} - 1$. Из равенства

$$2 \cdot (3 \cdot 2^{2^{n_1-1}-1} - 1) - 3 \cdot (2^{2^{n_1-1}} - 1) = 1$$

и критерия взаимной простоты целых чисел следует, что

$$(3 \cdot 2^{2^{n_1-1}-1} - 1, 2^{2^{n_1-1}} - 1) = 1. \quad (33)$$

Рассмотрим наибольший общий делитель чисел $3 \cdot 2^{2^{m-1}-1} - 1$ и $2^{2^{m-1}} + 1$.
Справедливо равенство

$$3 \cdot (2^{2^{m-1}} + 1) - 2 \cdot (3 \cdot 2^{2^{m-1}-1} - 1) = 5. \quad (34)$$

Найдем наибольший общий делитель чисел $2^{2^{m-1}} + 1$ и 5. Используя свойства наибольшего общего делителя целых чисел с учетом того, что $(2^t - 1, 2^t + 1) = 1$ для любого натурального t , получим последовательность равенств

$$\begin{aligned} (2^{2^{m-1}} + 1, 5) &= (2^{2^{m-1}} + 1, 2^2 + 1) = \\ &= \frac{(2^{2^m} - 1, 2^2 + 1)}{(2^{2^{m-1}} - 1, 2^2 + 1)} = \frac{(2^{2^m} - 1, 2^4 - 1)}{(2^{2^m} - 1, 2^2 - 1)} \cdot \frac{(2^{2^{m-1}} - 1, 2^2 - 1)}{(2^{2^{m-1}} - 1, 2^4 - 1)}. \end{aligned}$$

Отсюда, согласно (30),

$$(2^{2^{m-1}} + 1, 5) = \frac{2^{2(2^{m-1}, 2)} - 1}{2^2 - 1} \cdot \frac{2^{(2^{m-1}, 2)} - 1}{2^{(2^{m-1}, 4)} - 1}. \quad (35)$$

Из неравенства (32) и равенства (35) следует, что

$$(2^{2^{m-1}} + 1, 5) = 1. \quad (36)$$

Тогда из равенств (34) и (36) получим соотношение

$$(3 \cdot 2^{2^{m-1}-1} - 1, 2^{2^{m-1}} + 1) = 1. \quad (37)$$

В силу (33) и (37)

$$(3 \cdot 2^{2^{m-1}-1} - 1, 2^{2^m} - 1) = 1. \quad (38)$$

Так как

$$\begin{aligned} (3 \cdot 2^{2^{m-1}-1} - 1)^2 &= 9 \cdot 2^{2^m-2} - 6 \cdot 2^{2^{m-1}-1} + 1 = 2 \cdot 2^{2^m} + 2^{2^m-2} - 3 \cdot 2^{2^{m-1}} + 1 = \\ &= 2 \cdot (2^{2^m} - 1) + 2^{2^m-2} - 3 \cdot 2^{2^{m-1}} + 2 + 1 = 2 \cdot (2^{2^m} - 1) + 2^{2^m-2} - 2^{2^{m-1}+2} + 2^{2^{m-1}} + 2 + 1, \end{aligned}$$

то с учетом неравенства (32) получим, что остаток от деления числа $(3 \cdot 2^{2^{m-1}-1} - 1)^2$ на $2^{2^m} - 1$ равен $2^{2^{m-1}+2} \cdot (2^{2^{m-1}-4} - 1) + 2^{2^{m-1}} + 2 + 1$. Таким обра-

зом, двоичный вес остатка от деления числа $(3 \cdot 2^{2^{n_1-1}-1} - 1)^2$ на $2^{2^{n_1}} - 1$ равен $2^{n_1-1} - 1$. Отсюда и из равенства (38) следует, что при $n_2 = 1$ в качестве d' можно выбрать $3 \cdot 2^{2^{n_1-1}-1} - 1$. Лемма доказана.

ЗАМЕЧАНИЕ 5. Непосредственной проверкой можно установить, что для числа $n \leq 4$ не существует значений $d \in \{1, \dots, 2^n - 2\}$, удовлетворяющих условию леммы 1.

Лемма 2. Пусть n — натуральное число и τ — такая нечетная подстановка на множестве $\mathbb{F}_{2^n} \setminus \{0\}$, что τ^2 не принадлежит $\chi^{-1}(\text{GL}(n, 2))$. Тогда τ в объединении с $\chi^{-1}(\text{GL}(n, 2))$ в их действии на $\mathbb{F}_{2^n} \setminus \{0\}$ порождает группу $S(\mathbb{F}_{2^n} \setminus \{0\})$.

Доказательство. Заметим, что подстановка $\chi(\tau)$ является нечетной в группе $S((\mathbb{F}_2)^n \setminus \{\bar{0}\})$, а подстановка $\chi(\tau^2)$ является четной в группе $S((\mathbb{F}_2)^n \setminus \{\bar{0}\})$ и не лежит в группе $\text{GL}(n, 2)$. Согласно [6], группа $\text{GL}(n, 2)$ является максимальной подгруппой в знакопеременной группе подстановок множества $(\mathbb{F}_2)^n \setminus \{\bar{0}\}$. Следовательно, подстановка $\chi(\tau)^2$ и группа $\text{GL}(n, 2)$ порождают знакопеременную группу $A((\mathbb{F}_2)^n \setminus \{\bar{0}\})$. В то же время, группа $A((\mathbb{F}_2)^n \setminus \{\bar{0}\})$ и подстановка $\chi(\tau)$ порождают группу $S((\mathbb{F}_2)^n \setminus \{\bar{0}\})$. Следовательно,

$$\langle \{\chi(\tau)\} \cup \text{GL}(n, 2) \rangle = S((\mathbb{F}_2)^n \setminus \{\bar{0}\}).$$

Так как отображение χ задает изоморфизм групп подстановок $S(\mathbb{F}_{2^n} \setminus \{0\})$ и $S((\mathbb{F}_2)^n \setminus \{\bar{0}\})$, то множество $\{\tau\} \cup \chi^{-1}(\text{GL}(n, 2))$ порождает группу $S(\mathbb{F}_{2^n} \setminus \{0\})$. Лемма доказана.

Утверждение 3. Для любого натурального числа $n > 4$ существует такое число $d \in \{1, \dots, 2^n - 2\}$, что действие подстановки π_d и множества $\chi^{-1}(\text{GL}(n, 2))$ на $\mathbb{F}_{2^n} \setminus \{0\}$ порождает группу $S(\mathbb{F}_{2^n} \setminus \{0\})$.

Доказательство. Возьмем в качестве d любое число, удовлетворяющее условию леммы 1, и воспользуемся результатом леммы 2 при $\tau = \pi_d$. Утверждение доказано.

Следствие 1. Для любого натурального числа $n > 4$ действие группы $\mathcal{D}_n$ и множества $\chi^{-1}(\mathrm{GL}(n, 2))$ на $\mathbb{F}_{2^n} \setminus \{0\}$ порождает группу $S(\mathbb{F}_{2^n} \setminus \{0\})$.

Теорема 4. Для любого четного числа $n > 2$ класс гипер-бент-функций не замкнут относительно действия преобразований из полной линейной группы на аргумент функции.

Доказательство. Пусть натуральное число n больше двух и четно, а бент-функция $F' \in \mathcal{F}_n$ сохраняет нуль и является гипер-бент-функцией. Так как $F'(x)$ — бент-функция, то существует такой элемент $\beta \in \mathbb{F}_{2^n} \setminus \{0\}$, что вес функции $F'(x) + \mathrm{tr}_1^n(\beta x)$ совпадает с весом функции $F'(x)$. В этом случае справедливо равенство

$$\Delta(F'(x), \mathrm{tr}_1^n(\beta x)) = \Delta(F'(x), 0).$$

Согласно теореме 3, все мономы редуцированного многочлена приведенного представления функции $F'(x)$ имеют индекс нелинейности $n/2$. С другой стороны, отображение $F'' \in \mathcal{F}_n$, определяемое для любого элемента $x \in \mathbb{F}_{2^n}$ равенством

$$F''(x) = F'(x) + \mathrm{tr}_1^n(\beta x),$$

не является гипер-бент-функцией, так как его приведенное представление содержит моном индекса нелинейности, отличного от $n/2$. Однако функция F'' является бент-функцией в силу того, что для любого элемента $\alpha \in \mathbb{F}_{2^n}$ выполнено

$$\left| \Delta(F''(x), \mathrm{tr}_1^n(\alpha x)) \right| = \left| \Delta(F'(x), \mathrm{tr}_1^n((\alpha + \beta)x)) \right| = 2^{n/2}.$$

Кроме того, функции F' и F'' имеют одинаковый вес.

Рассмотрим два случая: $n = 4$ и $n > 4$.

1) Пусть n равно 4. Известно (см., например, [5, 17]), что все бент-функции от четырех переменных, сохраняющие нуль и имеющие одинаковый

вес, линейно эквивалентны. Следовательно, существует такая подстановка $l \in \text{GL}(4, 2)$, что

$$F''(x) = F'(\chi^{-1}(l)(x))$$

для всех элементов $x \in \mathbb{F}_{2^n} \setminus \{0\}$. Таким образом, класс гипер-бент-функций из множества $\mathcal{F}_4$ не замкнут относительно действия преобразований из полной линейной группы на аргумент функции.

2) Пусть теперь n — произвольное четное натуральное число, большее четырех. Так как функции F' и F'' сохраняют нуль и имеют одинаковый вес, то существует такая подстановка μ на множестве $\mathbb{F}_{2^n} \setminus \{0\}$, что для любого элемента $x \in \mathbb{F}_{2^n}$ выполнено равенство

$$F'(\mu(x)) = F''(x).$$

Согласно следствию 1, существуют такие натуральные числа t и не обязательно различные $d_1, \dots, d_t$, для которых $(d_i, 2^n - 1) = 1, i \in \{1, \dots, t\}$, и такие подстановки $l_1, \dots, l_t \in \text{GL}(n, 2)$, что имеет место равенство

$$\mu = \chi^{-1}(l_t) \circ \pi_{d_t} \circ \chi^{-1}(l_{t-1}) \circ \pi_{d_{t-1}} \circ \dots \circ \chi^{-1}(l_1) \circ \pi_{d_1}.$$

Рассмотрим конечную процедуру.

Шаг 1. Полагаем

$$F'_1(x) = F'(\pi_{d_1}(x))$$

для всех элементов $x \in \mathbb{F}_{2^n} \setminus \{0\}$, и

$$F'(0) = 0.$$

Из равенства (28) и замечания 3 следует, что функция F'_1 является гипер-бент-функцией. Полагаем

$$F''_1(x) = F'_1(\chi^{-1}(l_1)(x))$$

для всех элементов $x \in \mathbb{F}_{2^n} \setminus \{0\}$, и

$$F''_1(0) = 0.$$

Если функция F''_1 является гипер-бент-функцией, то перейдем к шагу 2. В противном случае останавливаем выполнение процедуры.

Шаг i (для $i \geq 2$). Полагаем

$$F'_i(x) = F''_{i-1}(\pi_{d_i}(x))$$

для всех элементов $x \in \mathbb{F}_{2^n} \setminus \{0\}$, и

$$F'_i(0) = 0.$$

Полагаем

$$F''_i(x) = F'_i(\chi^{-1}(l_i)(x)) \quad (39)$$

для всех элементов $x \in \mathbb{F}_{2^n} \setminus \{0\}$, и

$$F''_i(0) = 0.$$

Если F''_i — гипер-бент-функция, то переходим к шагу $i+1$. В противном случае останавливаем выполнение процедуры.

Заметим, что если в процессе выполнения процедуры был осуществлен переход к шагу i , то это означает, что на предыдущих шагах были найдены функции F'_j , F''_j , $j = \{1, \dots, i-1\}$, сохраняющие нуль и удовлетворяющие для всех элементов $x \in \mathbb{F}_{2^n} \setminus \{0\}$ равенствам

$$F'_j(x) = F''_{j-1}(\pi_{d_j}(x)), F''_j(x) = F'_j(\chi^{-1}(l_j)(x)), j = \{2, \dots, i-1\}.$$

Все эти функции являются гипер-бент-функциями. Если выполнение процедуры не было остановлено на шаге с номером, меньшим t , то это произойдет на шаге с номером t , так как для любого $x \in \mathbb{F}_{2^n}$ выполнено равенство $F''_t(x) = F''(x)$, а F'' не является гипер-бент-функцией.

Пусть выполнение процедуры остановлено на шаге с номером i . Тогда функция F'_i является гипер-бент-функцией, а функция F''_i не является гипер-бент-функцией. Но условие (39) означает, что эти функции могут быть получены одна из другой с помощью обратимого линейного преобразования векторного пространства $(\mathbb{F}_{2^n})_{\mathbb{F}_2}$. Следовательно, если n — произвольное четное натуральное число, большее четырех, то множество гипер-бент-функций из $\mathcal{F}_n$ не замкнуто относительно действия преобразований из полной линейной группы на аргумент функции. Теорема доказана.

ЗАМЕЧАНИЕ 6. В случае $n = 4$ справедлив более сильный результат: для любой гипер-бент-функции F из множества $\mathcal{F}_4$ существует такая подстанов-

ка $l \in \chi^{-1}(\text{GL}(4, 2))$, что отображение $F(l(x))$ не является гипер-бент-функцией.

Таким образом, в работе для любого четного $n > 2$ показана незамкнутость класса всех гипер-бент-функций из множества $\mathcal{F}_n$ и его подкласса $\mathcal{PS}_{ap}^{\#, 0}(n)$ относительно действия преобразований из полной линейной группы на аргумент функции.

Автор благодарен профессору Кузьмину А. С. за постановку задачи.

Список литературы

1. Кузьмин А. С., Марков В. Т., Нечаев А. А., Шишков А. Б. Приближение булевых функций мономиальными // Дискретная математика. — 2006. — Т. 18. № 1. — С. 9–29.
2. Кузьмин А. С., Нечаев А. А., Шишкин В. А. Бент- и гипер-бент-функции над полем из 2^l элементов // В сб.: Труды по дискретной математике, т. 18. — М.: ФИЗМАТЛИТ, 2006. — С. 86–111.
3. Логачев О. А., Сальников А. А., Яценко В. В. О свойствах сумм Вейля на конечных полях и конечных абелевых группах // Дискретная математика. — 1999. — Т. 11. № 2. — С. 66–85.
4. Логачев О. А., Сальников А. А., Яценко В. В. Булевы функции в теории кодирования и криптологии. — М.: МНЦМО, 2004. — 469 с.
5. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. Теория кодов, исправляющих ошибки. — М.: Связь, 1979. — 744 с.
6. Погорелов Б. А. О максимальных подгруппах симметрических групп, заданных на проективных пространствах над конечным полем // Математические заметки. — 1974. — Т. 26. № 1. — С. 91–100.
7. Сачков В. Н. Введение в комбинаторные методы дискретной математики. — М.: МЦНМО, 2004. — 424 с.
8. Токарева Н. Н. Нелинейные булевы функции: бент-функции и их обобщения. — LAP LAMBERT Acad. Publ. Saarbrücken, Germany, 2011. — 170 с.
9. Carlet C., Gaborit P. Hyper-bent-functions and cyclic codes // J. Comb. Theory. Ser. A. — 2006. — V. 113. — P. 466–482.
10. Carlitz L., Uchiyama S. Bounds for exponential sums // Duke Math. J. — 1957. — V. 24. — P. 37–41.
11. Dillon J. F. A survey of bent functions // The NSA Technical Journal. — 1972. — P. 191–215.
12. Dillon J. F. Elementary Hadamard difference sets. Ph. D. Thesis, Univ. of Maryland. — 1974.

13. *Gong G., Golomb S. W.* Transform domain analysis of DES // IEEE Trans. Inf. Theory. — 1999. — V. 45. № 6. — P. 2065–2073.
14. *Hou X.-D.* Cubic bent functions // Discrete Mathematics. — 1998. — V. 189. — P. 149–161.
15. *Langevin P., Leander G.* Classification of Boolean quartics forms in eight variables // Boolean Functions in Cryptology and Information Security. — 2008 — V. 18. — P. 139–147.
16. *Nyberg K.* Differentially uniform mappings for cryptography // EUROCRYPT'93 // Lect. Notes Comput. Sci. — 1994. — V. 765. — P. 55–64.
17. *Rothaus O. S.* On «bent» functions // J. Comb. Theory. Ser. A. — 1976. — V. 20. — P. 300–305.
18. *Youssef A., Gong G.* Hyper-bent functions // EUROCRYPT'2001 // Lect. Notes Comput. Sci. — 2001. — V. 2045. — P. 406–419.