2012 Теоретические основы прикладной дискретной математики №3(17)

DOI 10.17223/20710410/17/3

УДК 519.719.325

О СОВПАДЕНИИ КЛАССА БЕНТ-ФУНКЦИЙ С КЛАССОМ ФУНКЦИЙ, МИНИМАЛЬНО БЛИЗКИХ К ЛИНЕЙНЫМ[1]

В. И. Солодовников

Академия криптографии Российской Федерации, г. Москва, Россия

E-mail: vis0707@rambler.ru

Продолжается начатое ранее исследование вопросов близости функций из $(\mathbb{Z}/(p))^n$ в $(\mathbb{Z}/(p))^m$ (p — простое) к линейным функциям. Найдены новые критерии абсолютно минимальной близости функции к линейным. Доказывается, что такая минимальность функции наследуется её гомоморфными образами. Обобщая хорошо известный для булевых функций факт, доказывается, что для $p = 2, 3$ класс всех абсолютно минимально близких к линейным функций совпадает с классом бент-функций.

Ключевые слова: *близость функций, абсолютно негомоморфные функции, минимальные функции, бент-функции.*

Нам потребуются следующие обозначения, терминология и результаты работы [1]:

- X, Y — нетривиальные аддитивные конечные абелевы группы;
- Y^X — множество всех отображений $f : X \to Y$ из множества X в множество Y (термины «отображение» и «функция» считаем синонимами);
- $\psi\varphi$ — композиция отображений, при которой φ действует первым;
- $\mathrm{Hom}(G, H)$ — множество всех гомоморфизмов группы G в группу H;
- $\mathbb{Z}$ — кольцо целых чисел, $\mathbb{Z}/(k)$ — кольцо вычетов по модулю k;
- P — равномерное вероятностное распределение на X, то есть

$$P(A) = |A||X|^{-1} \text{ для любого } A \subseteq X.$$

Функция $f : X \to Y$ называется *сбалансированной*, если мощности полных прообразов всех элементов Y одинаковы.

В работе [1] близость двух произвольных функций $f_1, f_2 \in Y^X$ измеряется корнем из дисперсии

$$(|Y|^{-1} \sum_{y \in Y} (P(f_1 - f_2 = y) - |Y|^{-1})^2)^{\frac{1}{2}}.$$

В работе [2] предложено нормировать эту величину так, чтобы она достигала 1, то есть в качестве меры близости функций рассматривать

$$(|Y|(|Y| - 1)^{-1} \sum_{y \in Y} (P(f_1 - f_2 = y) - |Y|^{-1})^2)^{\frac{1}{2}}.$$

Это позволило упростить многие формулы. С целью дальнейших упрощений здесь мы откажемся и от корня. А именно, *близостью* δ функций $f_1, f_2 \in Y^X$ определим равенством

$$\delta(f_1, f_2) = |Y|(|Y| - 1)^{-1} \sum_{y \in Y} (P(f_1 - f_2 = y) - |Y|^{-1})^2, \tag{1}$$

[1]Работа выполнена в рамках НИР, проведённой в Академии криптографии Российской Федерации в 2010 г., и является расширенным вариантом статьи (добавлены теорема 5 и второй абзац снизу до списка литературы, изменены некоторые обозначения), опубликованной в журнале «Математические вопросы криптографии», 2011, т. 2, вып. 4, с. 97–108.

а близость классов функций $K_1, K_2 \subseteq Y^X$ — равенством

$$\delta(K_1, K_2) = \max_{\substack{f_1 \in K_1, \\ f_2 \in K_2}} \delta(f_1, f_2).$$

Близость δ обладает следующими свойствами:

$$0 \leqslant \delta(f_1, f_2) \leqslant 1; \tag{2}$$

$$\delta(f_1, f_2) = 0 \Leftrightarrow f_1 - f_2 \text{— сбалансированная}; \tag{3}$$

$$\delta(f_1, f_2) = 1 \Leftrightarrow f_1 - f_2 = \text{const}; \tag{4}$$

$$\delta(f_1, f_2) = \delta(f_2, f_1); \tag{5}$$

$$\delta(y_1 + g_2 f_1 g_1 + f', y_2 + g_2 f_2 g_1 + f') = \delta(f_1, f_2) \tag{6}$$

для любых $f_1, f_2 \in Y^X$, *сбалансированной* $g_1 : X' \to X$, изоморфизма $g_2 : Y \to Y'$, $f' : X' \to Y'$, $y_1, y_2 \in Y'$.

Свойства (2)–(4) означают, что минимально близкие функции — это функции, разность которых сбалансирована, а максимально близкие функции — это функции, разность которых есть константа.

Для любого $a \in X$ подстановку $x \mapsto a + x$ множества X будем обозначать через a^+. Все такие подстановки называют *сдвигами* группы X. Они образуют изоморфную группе X группу подстановок, называемую группой сдвигов (или группой Кэли) группы X (в теории представлений групп такое представление X называют регулярным).

Гомоморфизмы $h \in \mathrm{Hom}(X, Y)$ по определению обладают следующим характерным свойством: $ha^+ - h = \text{const}$ для всех $a \in X \setminus \{0\}$. Поэтому естественным (в силу свойств (2)–(4)) является следующее определение, обобщающее определение «совершенной нелинейности» в [3].

Функция $f : X \to Y$ называется *абсолютно негомоморфной*, если для любого $a \in X \setminus \{0\}$ функция $fa^+ - f$ является сбалансированной, то есть

$$\delta(fa^+, f) = 0. \tag{7}$$

Множество всех абсолютно негомоморфных функций из Y^X обозначается через $AN(Y^X)$. В частности, $AN(Y^X) = \varnothing$ при $|X| < |Y|$.

К понятию абсолютной негомоморфности можно подойти не только с алгебраической, но и с криптографической стороны. А именно, пусть G — некоторая группа подстановок множества X, $fG = \{fg : g \in G\}$ — класс функций, порождённых функцией $f \in Y^X$ и группой G. Пусть в некоторой криптосхеме имеется узел, реализующий функции из fG, где элементы группы G являются ключами. Тогда величины $\delta(fg_1, fg_2)$, $g_1, g_2 \in G$, характеризуют степень изменения этого узла ключами из G: чем ближе эти величины к 0, тем сильнее подстановки из G изменяют функцию f. Наоборот, если величина $\delta(fg_1, fg_2)$ близка к 1, то ключи g_1 и g_2 называют *близкими*. Поскольку, в силу (6), $\delta(fg_1, fg_2) = \delta(fg_1 g_2^{-1}, f)$, то достаточно рассматривать только величины $\delta(fg, f)$, $g \in G$. В частности, когда G — группа сдвигов группы X, получаем, что абсолютно негомоморфные функции — это функции, которые *максимально изменяются сдвигами*, то есть соответствующие узлы *не имеют различных близких ключей-сдвигов*.

В работе [1] доказано, что если группа G транзитивна, то для любой $f \in Y^X$

$$\delta(f, 0) = |Y|(|G|(|Y| - 1))^{-1} \sum_{g \in G} (P(fg = f) - |Y|^{-1})$$

и, в частности, для любого $h \in \mathrm{Hom}(X, Y)$

$$\delta(f, h) = |Y|(|X|(|Y| - 1))^{-1} \sum_{a \in X} (P(fa^+ - f = h(a)) - |Y|^{-1}). \tag{8}$$

Приведём некоторые свойства абсолютно негомоморфных функций.

Если $f \in AN(Y^X)$, $h \in \mathrm{Hom}(X, Y)$, $g_1 : X' \to X$ — изоморфизм, $g_2 : Y \to Y'$ — эпиморфизм (сюръективный гомоморфизм групп), $c \in X'$, $b \in Y'$, $h' \in \mathrm{Hom}(X', Y')$, то

$$\delta(f, h) = |X|^{-1}; \tag{9}$$

$$b + h' + g_2 f g_1 c^+ \in AN(Y'^{X'}). \tag{10}$$

Из формулы (9) следует, что абсолютно негомоморфные функции одинаково близки к любому гомоморфизму, а также что они не являются сбалансированными, поскольку сбалансированность равносильна условию $\delta(f, 0) = 0$. В частности, абсолютно негомоморфные функции не могут быть биективными.

В соответствии с теоретико-автоматной терминологией и с учетом групповой структуры алфавитов, пару (α, β) гомоморфизмов $\alpha \in \mathrm{Hom}(X, X')$ и $\beta \in \mathrm{Hom}(Y, Y')$ назовем *гомоморфизмом функции* $f : X \to Y$ *в функцию* $f' : X' \to Y'$, если $\beta f = f'\alpha$. Если α и β — сюръекции, то гомоморфизм (α, β) назовем эпиморфизмом, а функцию f' — гомоморфным образом функции f. В этом случае для любых $a \in X$ и $y' \in Y'$

$$P'(f'(\alpha(a))^+ - f' = y') - |Y'|^{-1} = \sum_{y \in \beta^{-1}(y')} (P(fa^+ - f = y) - |Y|^{-1}), \tag{11}$$

где $P'(A') = |A'||X'|^{-1}$ для любого $A' \subseteq X'$, и следовательно, справедлива

Теорема 1. Если (α, β) — эпиморфизм функции $f \in AN(Y^X)$ в функцию $f' : X' \to Y'$ и $|Y'| > 1$, то α — изоморфизм и $f' \in AN(Y'^{X'})$.

Минимальная близость функций из Y^X к гомоморфизмам обозначается через

$$\delta_0(Y^X) = \min_{f \in Y^X} \delta(f, \mathrm{Hom}(X, Y)).$$

Минимальными называются функции, минимально близкие к гомоморфизмам, то есть функции $f \in Y^X$, для которых

$$\delta(f, \mathrm{Hom}(X, Y)) = \delta_0(Y^X).$$

Множество всех минимальных функций из Y^X обозначим через $M(Y^X)$.

Заметим, что минимальные функции существуют всегда, в отличие от абсолютно негомоморфных функций.

Хорошо известно, что любая абелева группа изоморфна прямому произведению аддитивных групп колец вычетов. Поэтому, и в силу формул (6) и (10), без ограничения общности далее считаем, что

$$X = \prod_{i=1}^{n} \mathbb{Z}/(k_i),\ Y = \prod_{j=1}^{m} \mathbb{Z}/(t_j),$$

где n, m — произвольные натуральные числа, $k_1, \ldots, k_n$, $t_1, \ldots, t_m$ — произвольные большие 1 натуральные числа.

В работе [1] для функций из Y^X введено понятие *бент-функции* как функции, обладающей следующим свойством: в разложении композиции её и любого неединичного

неприводимого (комплекснозначного) характера группы Y по неприводимым характерам группы X модули всех коэффициентов (они называются коэффициентами Фурье) одинаковы. Множество всех бент-функций из Y^X обозначим через $B(Y^X)$.

Это определение обобщает определения работы [4] (для булевых функций, то есть $m = 1$, $k_1 = \ldots = k_n = t_1 = 2$), работы [5] (для $k_1 = \ldots = k_n = t_1 = \ldots = t_m = p$ — простое число, m делит n) и может быть сведено к определению работы [6], где бент-функции определяются как комплекснозначные функции на конечной абелевой группе с единичными модулями всех значений и условием равенства модулей всех коэффициентов Фурье. Для случая $m = 1$, $k_1 = \ldots = k_n = t_1 \geqslant 3$ определение из [1] сужает определение бент-функции в [7] (где участвует только один характер группы Y), но в [7] доказано, что при простом t_1 эти определения равносильны. В замечательной книге [8] приводится обстоятельный обзор бент-тематики.

В [1] доказано:

$$AN(Y^X) = B(Y^X),$$

что распространяет соответствующие результаты работ [4, 5, 7] на случай произвольных конечных абелевых групп X и Y.

Для любого $h \in \mathrm{Hom}(X, Y)$ *матрица гомоморфизма* h

$$A_h = (a_{i,j} + (t_j))_{n \times m}$$

определяется равенствами

$$h(e_i) = (a_{i,1} + (t_1), \ldots, a_{i,m} + (t_m)),$$
$$e_i = ((k_1), \ldots, (k_{i-1}), 1 + (k_i), (k_{i+1}), \ldots, (k_n)),\ i = 1, \ldots, n.$$

Она обладает следующими свойствами:

$$\frac{t_j}{(k_i, t_j)} \mid a_{i,j} \tag{12}$$

для любых $i = 1, \ldots, n$, $j = 1, \ldots, m$ (здесь (k_i, t_j) — наибольший общий делитель чисел k_i и t_j, а $a \mid b$ обозначает, что a делит b),

$$h((x_1 + (k_1), \ldots, x_n + (k_n))) = (x_1, \ldots, x_n)A_h$$

для любых $x_1, \ldots, x_n \in \mathbb{Z}$. Следовательно, матрица A_h однозначно определяет сам гомоморфизм h. Наоборот, если $A = (a_{i,j} + (t_j))_{n \times m}$ — произвольная матрица со свойством (12), то соответствие $h_A : X \to Y$, определяемое равенством

$$h_A((x_1 + (k_1), \ldots, x_n + (k_n))) = (x_1, \ldots, x_n)A,$$

является гомоморфизмом групп. Таким образом, между $\mathrm{Hom}(X, Y)$ и всеми матрицами со свойством (12) существует взаимно-однозначное соответствие и, следовательно,

$$|\mathrm{Hom}(X, Y)| = \prod_{\substack{i=1,\ldots,n,\\ j=1,\ldots,m}} (k_i, t_j).$$

Следующая, доказанная в [1], теорема распространяет известный результат работы [9] для булевых функций на случай абелевых групп.

Теорема 2. Если $k_i | t_j$ для любых $i = 1, \ldots, n$, $j = 1, \ldots, m$, то для любой функции $f : X \to Y$ набор чисел

$$(P(f = y + h) : y \in Y, h \in \mathrm{Hom}(X, Y))$$

однозначно определяет функцию f.

Следующие две теоремы (см. [1, 3]) сводят случай многомерного Y к одномерному и обобщают теорему 3 из [5].

Теорема 3. Если $k_i = t_j = t$ для любых $i = 1, \ldots, n$, $j = 1, \ldots, m$, то для любой $f : X \to Y$ следующие свойства равносильны:

1) f — сбалансированная;

2) hf — сбалансированная для любого эпиморфизма $h : Y \to \mathbb{Z}/(t)$.

Теорема 4. Если $k_i = t_j = t$ для любых $i = 1, \ldots, n$, $j = 1, \ldots, m$, то для любой $f : X \to Y$ следующие свойства равносильны:

1) $f \in B(Y^X)$;

2) $hf \in B(\mathbb{Z}/(t)^X)$ для любого эпиморфизма $h : Y \to \mathbb{Z}/(t)$.

Лемма 1. Следующие свойства равносильны:

а) для любых $x \in X \backslash \{0\}$, $y \in Y$ существует $h \in \mathrm{Hom}(X, Y)$, такой, что $h(x) = y$;

б) $k_1 = \ldots = k_n = t_1 = \ldots t_m = p$ — простое число.

Доказательство. Импликация *б* $\Rightarrow$ *а* очевидна, так как в случае *б* гомоморфизмы являются линейными отображениями (функциями) векторных пространств над полем $\mathbb{Z}/(p)$. Наоборот, пусть выполнено *а*. Тогда, в силу (12), $t_j \mid k_i$ для любых $i = 1, \ldots, n$, $j = 1, \ldots, m$. Для любого $h \in \mathrm{Hom}(X, Y)$ в $h(t_j e_i)$ j-я координата равна 0 и, следовательно, $t_j = k_i = p = c_1 c_2$, где $c_1 > 1$. Тогда $c_1 h(c_2 e_1) = 0$ для любого $h \in \mathrm{Hom}(X, Y)$ и, следовательно, $c_2 = 1$. ■

Условие *а* существенно для дальнейших рассуждений. Поэтому далее рассмотрим только случай выполнения условия *б* леммы 1, $p > 1$, который назовем *примарным* (или *p-примарным*), при этом функции из Y^X — *примарными* (или *p-примарными*). В этом случае гомоморфизмы из $\mathrm{Hom}(X, Y)$ являются линейными функциями (отображениями векторных пространств) и

$$|\mathrm{Hom}(X, Y)| = |Y|^n = p^{nm}.$$

2-Примарный случай называют двоичным. Двоичный случай для $m = 1$ называют булевым. С практической точки зрения оба эти случая наиболее интересны.

Теорема 5. Для p-примарного случая следующие утверждения равносильны:

1) $B(Y^X) \neq \varnothing$;

2) выполняется одно из условий:

$$p = 2, \;\; 2 \,|\, n \text{ и } n \geqslant 2m,$$
$$p \geqslant 3 \text{ и } n \geqslant m.$$

Доказательство. В [3, 5] указаны следующие два примера абсолютно негомоморфных функций. Если $2 \,|\, n$, то операция умножения в поле $\mathrm{GF}(p^{n/2})$ является абсолютно негомоморфной функцией $\mathrm{GF}(p^{n/2})^2 \to \mathrm{GF}(p^{n/2})$. Если $p \geqslant 3$, то возведение в квадрат в поле $\mathrm{GF}(p^n)$ является абсолютно негомоморфной функцией $\mathrm{GF}(p^n) \to \mathrm{GF}(p^n)$. Отсюда и из свойства (10) следует справедливость импликации $2 \Rightarrow 1$.

Наоборот, пусть выполнено утверждение 1. Тогда, по определению сбалансированности, $n \geqslant m$. Пусть $p = 2$. В [3] доказано, что если $f : X \to Y$ — бент-функция, то мощность полного прообраза любого $y \in Y$ при отображении f равна $2^{n/2-m}k(f, y)$, где $k(f, y)$ — нечётное число (в частности, любая двоичная бент-функция сюръективна). ■

В [1] доказана

Лемма 2. Для любой примарной $f : X \to Y$

$$|Y|^{-n} \sum_{h \in \mathrm{Hom}(X,Y)} \delta(f, h) = |X|^{-1}.$$

Доказательство. Приводимое ниже доказательство проще, чем в [1], и не использует коэффициенты Фурье.

Для любого $a \in X\backslash\{0\}$ отображение $\mathrm{Hom}(X, Y) \to Y$, где $h \mapsto h(a)$, является гомоморфизмом групп, который сюръективен в силу леммы 1. Тогда, в силу (8),

$$|Y|^{-n} \sum_{h \in \mathrm{Hom}(X,Y)} \delta(f, h) =$$

$$= |Y|^{-n}|Y|(|X|(|Y| - 1))^{-1}(|Y|^n(1 - |Y|^{-1}) + \sum_{0 \neq a \in X} \sum_{h \in \mathrm{Hom}(X,Y)} (P(fa^+ - f = h(a)) - |Y|^{-1})) =$$

$$= |Y|^{-n}|Y|(|X|(|Y| - 1))^{-1}(|Y|^n(1 - |Y|^{-1}) + (|X| - 1)(|Y|^{n-1}1 - |Y|^n|Y|^{-1})) = |X|^{-1}.$$

Лемма доказана. ■

Из этой леммы получаем оценку минимальной близости функций к линейным функциям.

Теорема 6. Для примарного случая

$$\delta_0(Y^X) \geqslant |X|^{-1}.$$

В случае выполнения условия $\delta_0(Y^X) = |X|^{-1}$ минимальные функции назовем *абсолютно минимальными* (в силу теоремы 9 это определение сужает определение «абсолютной минимальности» в работе [1]). Множество всех абсолютно минимальных функций из Y^X обозначим через $AM(Y^X)$, так что

$$M(Y^X) = AM(Y^X), \text{ если } \delta_0(Y^X) = |X|^{-1},$$
$$AM(Y^X) = \varnothing, \text{ если } \delta_0(Y^X) > |X|^{-1}.$$

Из формулы (9) и теоремы 6 следует

Теорема 7. В примарном случае $AN(Y^X) \subseteq AM(Y^X)$.

В следующей теореме собраны критерии абсолютной минимальности примарных функций.

Теорема 8. Для любой p-примарной $f : X \to Y$ следующие утверждения равносильны:

1) $f \in AM(Y^X)$;
2) $\delta(f, h) = |X|^{-1}$ для любого $h \in \mathrm{Hom}(X, Y)$;
3) $\delta(f, h) = \delta(f, h')$ для любых $h, h' \in \mathrm{Hom}(X, Y)$;
4) $\sum\limits_{0 \neq a \in X} (P(fa^+ - f = h(a)) - |Y|^{-1}) = 0$ для любого $h \in \mathrm{Hom}(X, Y)$;
5) $\sum\limits_{0 \neq a \in X} (P(fa^+ - f = h(a)) - |Y|^{-1}) = \sum\limits_{0 \neq a \in X} (P(fa^+ - f = h'(a)) - |Y|^{-1})$ для любых $h, h' \in \mathrm{Hom}(X, Y)$;

6) $\sum\limits_{0\neq c\in Z/(p)}(P(f(ca)^+ - f = cy) - |Y|^{-1}) = 0$ для любых $a \in X\backslash\{0\}$, $y \in Y$;

7) $\sum\limits_{0\neq c\in Z/(p)}(P(f(ca)^+ - f = cy) - |Y|^{-1}) = \sum\limits_{0\neq c\in Z/(p)}(P(f(ca)^+ - f = cy') - |Y|^{-1})$ для любых $a \in X\backslash\{0\}$, $y, y' \in Y$.

Доказательство. Импликация $1 \Rightarrow 2$ следует из определения минимальности и леммы 2. Очевидно, что $2 \Rightarrow 3$. Импликация $3 \Rightarrow 1$ следует из леммы 2, теоремы 6 и определения минимальности. Из формулы (8) следуют равносильности $2 \Leftrightarrow 4$ и $3 \Leftrightarrow 5$. Импликации $6 \Rightarrow 7$ и $7 \Rightarrow 5$ очевидны.

Осталось доказать $4 \Rightarrow 6$. При $n = 1$ импликация очевидна. Пусть $n \geqslant 2$ и $a_1, \ldots, a_n$ — любой базис пространства X. Для любых $y_1, \ldots, y_n \in Y$ определим $h_{y_1,\ldots,y_n} : X \to Y$ равенством $h_{y_1,\ldots,y_n}(a) = \sum\limits_{i=1}^{n} c_i y_i$ для всех $a = \sum\limits_{i=1}^{n} c_i a_i \in X$, $c_1, \ldots, c_n \in \mathbb{Z}/(p)$, так что $h_{y_1,\ldots,y_n} \in \mathrm{Hom}(X, Y)$. Тогда

$$
\begin{aligned}
0 = |Y|^{n-1}\cdot 0 &= \sum_{0\neq a\in X}\ \sum_{y_2,\ldots,y_n\in Y}(P(fa^+ - f = h_{y_1,\ldots,y_n}(a)) - |Y|^{-1}) = \\
&= \sum_{0\neq c_1\in\mathbb{Z}/(p)} |Y|^{n-1}(P(f(c_1a_1)^+ - f = c_1y_1) - |Y|^{-1}) + \\
&+ \sum_{\substack{\bar 0\neq(c_2,\ldots,c_n)\in(\mathbb{Z}/(p))^{n-1},\\ c_1\in\mathbb{Z}/(p)}}\ \sum_{y_2,\ldots,y_n\in Y}(P(fa^+ - f = \sum_{i=1}^{n} c_iy_i)) - |Y|^{-1}) = \\
&= |Y|^{n-1}\sum_{0\neq c_1\in\mathbb{Z}/(p)}(P(f(c_1a_1)^+ - f = c_1y_1) - |Y|^{-1}) + \\
&+ \sum_{\substack{\bar 0\neq(c_2,\ldots,c_n)\in(\mathbb{Z}/(p))^{n-1},\\ c_1\in\mathbb{Z}/(p)}}\ \sum_{y_2,\ldots,y_n\in Y}(P(fa^+ - f = c_1y_1 + \sum_{i=2}^{n} c_iy_i)) - |Y|^{-1}) = \\
&= |Y|^{n-1}\sum_{0\neq c_1\in\mathbb{Z}/(p)}(P(f(c_1a_1)^+ - f = c_1y_1) - |Y|^{-1}) + \\
&+ \sum_{\substack{\bar 0\neq(c_2,\ldots,c_n)\in(\mathbb{Z}/(p))^{n-1},\\ c_1\in\mathbb{Z}/(p)}} |Y|^{n-2}\sum_{y\in Y}(P(fa^+ - f = y) - |Y|^{-1}) = \\
&= |Y|^{n-1}\sum_{0\neq c_1\in\mathbb{Z}/(p)}(P(f(c_1a_1)^+ - f = c_1y_1) - |Y|^{-1}).
\end{aligned}
$$

Теорема доказана. ■

Теорема 1 означает, что свойство абсолютной негомоморфности (т. е. бентовости) наследуется гомоморфными образами, а также то, что бент-функции не имеют нетривиальных гомоморфных образов с $|X'| < |X|$. Покажем, что это справедливо и для свойства абсолютной минимальности.

Теорема 9. Если в примарном случае $f \in AM(Y^X)$, $f' : X' \to Y'$ — гомоморфный образ функции f и $|Y'| > 1$, то $|X'| = |X|$ и $f' \in AM(Y'^{X'})$.

Доказательство. Для любых $a \in X\backslash\{0\}$, $y' \in Y'$ по формуле (11)

$$\sum_{0\neq c\in\mathbb{Z}/(p)}(P'(f'(c\alpha(a))^+ - f' = cy') - |Y'|^{-1}) = \sum_{0\neq c\in\mathbb{Z}/(p)}\ \sum_{y\in\beta^{-1}(y')}(P(f(ca)^+ - f = cy) - |Y|^{-1}) = 0$$

в силу утверждения 6 теоремы 8. Тогда α — изоморфизм, утверждение 6 теоремы 8 выполнено для X', Y', f' и теорема доказана. ■

Заметим, что теорема 9 для $Y' = \mathbb{Z}/(p)$ равносильна доказанному В. А. Шишкиным в 2008 г. некоторому свойству коэффициентов Фурье (результат не опубликован).

Следующая теорема обобщает хорошо известный для булевого случая факт (см., например, [4]).

Теорема 10. Для p-примарного случая, $p \in \{2, 3\}$, следующие утверждения равносильны:

1) $B(Y^X) \neq \varnothing$;
2) $\delta_0(Y^X) = |X|^{-1}$;
3) $B(Y^X) = M(Y^X)$.

Доказательство. Импликация $3 \Rightarrow 1$ очевидна; $1 \Rightarrow 2$ следует из теоремы 7. Докажем импликацию $2 \Rightarrow 3$. При $p = 2$ она следует из утверждения 6 теоремы 8. Пусть $p = 3$. Для любого p выполняются равенства

$$P(f(-ca)^+ - f = -cy) - |Y|^{-1} = P(f - f(ca)^+ = -cy) - |Y|^{-1} = P(f(ca)^+ - f = cy) - |Y|^{-1}.$$

Пусть f — минимальная. Тогда из утверждения 6 теоремы 8 получаем, что для любых $a \in X \backslash \{0\}$, $y \in Y$ имеет место

$$0 = \sum_{c \in \{1,-1\}} (P(f(ca)^+ - f = cy) - |Y|^{-1}) = 2(P(f(a)^+ - f = y) - |Y|^{-1}),$$

и, следовательно, f — абсолютно негомоморфная. ■

Отметим, что все приведённые доказательства не используют аппарат характеров абелевых групп и разложения Фурье.

В заключение введём следующие обозначения и терминологию.

Для любой $f : X \to Y$ обозначим

$$\bar{\delta}(f) = |X|^{-1} \sum_{a \in X} \delta(fa^+, f), \quad \delta_1(Y^X) = \min_{f \in Y^X} \bar{\delta}(f).$$

Максимально негомоморфными назовём функции $f \in Y^X$, для которых

$$\bar{\delta}(f) = \delta_1(Y^X).$$

Множество всех максимально негомоморфных функций из Y^X обозначим через $N(Y^X)$, так что $N(Y^X) \neq \varnothing$ и

$$N(Y^X) = AN(Y^X), \text{ если } \delta_1(Y^X) = |X|^{-1},$$
$$AN(Y^X) = \varnothing, \text{ если } \delta_1(Y^X) > |X|^{-1}.$$

Представляется справедливой следующая

Гипотеза. Для p-примарного случая и любого p

$$M(Y^X) = N(Y^X); \tag{13}$$
$$AM(Y^X) = AN(Y^X). \tag{14}$$

Заметим, что равенства (13) и (14) совпадают в том и только в том случае, когда $B(Y^X) \neq \varnothing$ (см. теорему 5).

Теорема 10 равносильна выполнению равенства (14) для $p \in \{2, 3\}$. В силу теорем 7, 9, 4 равенство (14) достаточно доказать для случая $m = 1$.

Заменяя в соответствующих определениях множество всех функций Y^X на произвольный класс функций $K \subseteq Y^X$, приходим к естественному и актуальному для приложений обобщению понятий минимальности и негомоморфности на случай функций из

класса K: $\delta_0(K)$, $\delta_1(K)$, $M(K)$, $N(K)$ (например, K — класс всех подстановок, $M(K)$ — минимальные подстановки, $N(K)$ — максимально негомоморфные подстановки).

Наконец, заметим, что, в отличие от приведённого выше общепринятого определения бент-функции (через равномодульность коэффициентов Фурье), в работе [2] для произвольного простого p и в работе [10] для $p = 2$ бент-функциями названы *абсолютно минимальные* функции. При этом, ссылаясь на работу [1], в [2, теорема 3.2] фактически утверждается, что теорема 10 справедлива для любого простого p (чего не удалось доказать автору ни здесь, ни в [1]). Последствием этого явилась необоснованность распространения некоторых свойств бент-функций на абсолютно минимальные функции. Однако теорема 10 теперь обосновывает такое распространение в работе [2] для случая $p = 2, 3$ и в работе [10]. Заметим, что основные результаты работы [2] относятся к случаю $p = 2$.

ЛИТЕРАТУРА

1. *Солодовников В. И.* Бент-функции из конечной абелевой группы в конечную абелеву группу // Дискретная математика. 2002. Т. 14. № 1. С. 99–113.
2. *Кузьмин А. С., Нечаев А. А., Шишкин В. А.* Бент- и гипербент-функции над конечным полем // Труды по дискретной математике. 2007. Т. 10. С. 97–122.
3. *Nyberg K.* Perfect nonlinear S-boxes // LNCS. 1991. V. 547. P. 378–386.
4. *Rothaus O. S.* On "bent" functions // J. Comb. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
5. *Амбросимов А. С.* Свойства бент-функций q-значной логики над конечными полями // Дискретная математика. 1994. Т. 6. № 3. С. 50–60.
6. *Логачёв О. А., Сальников А. А., Ященко В. В.* Бент-функции на конечной абелевой группе // Дискретная математика. 1997. Т. 9. № 4. С. 3–20.
7. *Kumar P. V., Scholts R. A., and Welch L. R.* Generalized bent functions and their properties // J. Comb. Theory. Ser. A. 1985. V. 40. No. 1. P. 90–107.
8. *Токарева Н. Н.* Нелинейные булевы функции: бент-функции и их обобщения. Saarbrucken, Germany: LAP LAMBERT Academic Publishing, 2011.
9. *Golomb S. W.* On the classification of Boolean functions // IRE Trans. Circuit Theory. 1959. V. 1. No. 6. P. 10–27.
10. *Кузьмин А. С., Нечаев А. А., Шишкин В. А.* Параметры (гипер-) бент-функций над полем из 2^l элементов // Труды по дискретной математике. 2008. Т. 11/1. С. 47–59.