Math-Net.Ru

Общероссийский математический портал

Б. А. Погорелов, М. А. Пудовкина, Орбитальные производные по подгруппами их комбинаторно-групповые свойства, *Дискрет. матем.*, 2015, том 27, выпуск 4, 94–119

DOI: <https://doi.org/10.4213/dm1350>

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: 18.234.156.22

26 апреля 2023 г., 12:31:25

Орбитальные производные по подгруппам и их комбинаторно-групповые свойства

© 2015 г. Б. А. Погорелов*, М. А. Пудовкина**

Рассматриваются свойства орбитальных производных по подгруппам группы G_n , порождённой аддитивными группами кольца вычетов $\mathbb{Z}_{2^n}$ и n -мерного векторного пространства V_n над полем $GF(2)$. Описываются неуплотняемые последовательности вложенных орбит для подгрупп группы G_n и силовой подгруппы P_n симметрической группы S_{2^n} . Для орбитальных производных рассматриваются три аналога понятия степени нелинейности для функций над $\mathbb{Z}_{2^n}$ или V_n .

Ключевые слова: аддитивная группа кольца вычетов, аддитивная группа векторного пространства, силовая 2-подгруппа, степень нелинейности, нормальные подгруппы

1. Введение

В криптографии производные дискретных отображений играют важную роль. Они используются в методах криптографического анализа, на их основе задаются криптографические параметры и вводятся целые классы отображений. Производная двоичной функции по направлению вектора v в группе инерции содержит сдвиг на этот вектор. Линейная структура двоичной функции также связана с группой сдвигов. Так, на орбитах каждого сдвига векторного пространства, принадлежащего линейной структуре, функция принимает одинаковые или противоположные значения.

Производные отображений и определяемые ими криптографические параметры рассматриваются, в основном, над n -мерным векторным пространством V_n над полем $GF(2)$. Свойствам производных над кольцом вычетов $\mathbb{Z}_{q^n}$, их заданию, учитывающему алгебраическую структуру кольца, а также криптографическим свойствам, до недавнего времени уделялось меньше внимания [7], [8], [9], [3], [4].

В [3], [4] рассматривались орбитальные производные функций над кольцом вычетов $\mathbb{Z}_{2^n}$. В этом случае производная i -го порядка определялась как сумма значений функции $f : \mathbb{Z}_{2^n} \rightarrow \mathbb{Z}_{2^m}$ на орбитах аддитивной группы $\langle 2^{n-i} \rangle$, порождённой

*Место работы: Академия криптографии Российской Федерации,
e-mail: pogorelow.b@yandex.ru

**Место работы: Национальный исследовательский ядерный университет (МИФИ),
e-mail: maricap@rambler.ru

элементом 2^{n-i} . В [5] предложено понятие орбитальной производной, обобщающее случай $q = 2$. Оно также основано на суммировании значений функции на орбитах ряда вложенных подгрупп неабелевой группы G_n , порожденной группами сдвигов векторного пространства V_n и кольца вычетов $\mathbb{Z}_{2^n}$.

В настоящей работе описываются неуплотняемые последовательности вложенных орбит для подгрупп группы G_n и силовской подгруппы P_n симметрической группы S_{2^n} . Это позволяет говорить о самых длинных последовательностях нетривиальных производных.

В терминах орбитальных производных приводятся три аналога понятия степени нелинейности для функций над $\mathbb{Z}_{2^n}$ и V_n , называемых степенями асимметричности. Для орбитальных производных по абелевым группам эти понятия совпадают. Первое из них, но для орбитальных производных, схоже с понятием степени нелинейности функций на абелевых группах, рассмотренным в [7], [8], [9]. Второе связано с неуплотняемой последовательностью вложенных орбит подгрупп групп G_n или P_n .

Третье связано с наибольшими и наименьшими длинами такой последовательности $\bar{H} = H_1, \dots, H_c$ вложенных подгрупп групп G_n , P_n , что орбитальные производные относительно всех элементов последовательности $\bar{H}$ попарно различны, а производная по подгруппе H_c является константным отображением. При рассмотрении нормальных подгрупп групп G_n , P_n данное определение совпадает с понятием Δ_+ -степени отображения, введенным в [3]. Приводятся оценки сверху степеней асимметричности для V_n и $\mathbb{Z}_{2^n}$. При этом обобщается ряд результатов, полученных в [3], [4].

2. Основные обозначения

Пусть $\mathbb{N}$ – множество всех натуральных чисел, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$; $\mathbb{Z}$ – кольцо целых чисел; $Z_m = \{0, \dots, m-1\} \subset \mathbb{Z}$; $\mathbb{Z}_{2^n}$ – кольцо вычетов по модулю 2^n , элементы которого обозначаются числами $0, \dots, 2^n - 1$; при $d \leq n$ для $\alpha \in \mathbb{Z}_{2^n}$ через $\alpha_{(d)}$ обозначаем такой элемент $\alpha_{(d)} \in \mathbb{Z}_{2^d}$, что $\alpha_{(d)} \equiv \alpha \pmod{2^d}$, при этом $\alpha_{(0)} = 0$, $x \mapsto x_{(d)}$ – соответствующее отображение; $A_{(d)} = \{\alpha_{(d)} | \alpha \in A\}$ для $A \subset \mathbb{Z}$; V_n – пространство n -мерных векторов над полем $GF(2)$, т.е. $V_n = (GF(2))^n$; $\oplus$ – операция покоординатного сложения векторов в пространстве V_n .

Каждый вектор $\alpha = (\alpha_{n-1}, \dots, \alpha_1, \alpha_0) \in V_n$ можно рассматривать и как двоичную запись числа $\tilde{\alpha} = 2^{n-1}\alpha_{n-1} + \dots + 2\alpha_1 + \alpha_0$. Поэтому вектор α будем отождествлять с числом $\tilde{\alpha}$. При этом на V_n можно определить операции сложения и умножения по модулю 2^n , а над кольцом $\mathbb{Z}_{2^n}$ – операцию $\oplus$ покоординатного сложения векторов. Эти операции будем обозначать теми же знаками, что и соответствующие операции над числами или векторами. Из контекста всегда будет ясно, о каких операциях идет речь и над какой алгебраической структурой.

Пусть также $\mathbb{Z}_{2^n}^+$ и V_n^+ – аддитивные группы кольца $\mathbb{Z}_{2^n}$ и векторного пространства V_n ; $H \leq R$ – H -подгруппа группы R ; $S(X)$ – симметрическая группа на множестве X , $S_{2^n} = S(X)$ при $|X| = 2^n$; $G_n = \langle V_n^+, \mathbb{Z}_{2^n}^+ \rangle \leq S_{2^n}$; P_n -силовская 2-подгруппа группы S_{2^n} , содержащая группу G_n ; e – тождественная подстановка; $\alpha^g = \alpha g = g(\alpha)$ – образ элемента $\alpha \in X$ при действии на него подстановкой $g \in S(X)$;

$\alpha^G = \{\alpha^g \mid g \in G\}$, $G \leq S(X)$; $X^\times = X \setminus \{0\}$, если 0 – нейтральный элемент относительно заданной на X бинарной операции; $A * B = \{\alpha * \beta \mid (\alpha, \beta) \in A \times B\}$ для группы X с бинарной операцией $*$, $A, B \subset X$, B^c – c -я декартова степень множества B ; $\langle \beta_1, \dots, \beta_t \rangle$ – группа, порождённая элементами $\beta_1, \dots, \beta_t$; $F_{n,m}^+ = \{f \mid f: \mathbb{Z}_{2^n} \rightarrow \mathbb{Z}_{2^m}\}$, $F_{n,m}^\oplus = \{f \mid f: V_n \rightarrow V_m\}$ при $1 \leq m \leq n$; $a(x) \cdot b(x) \equiv_{2^m} c(x)$ есть сокращённая запись условия $a(x) \cdot b(x) \equiv c(x) \pmod{2^m}$ для всех $x \in \mathbb{Z}_{2^n}$, где $a, b, c \in F_{n,m}^+$, « $\cdot$ » – бинарная операция над числами в кольце $\mathbb{Z}$, представляющими соответствующие классы вычетов; запись $a *_{2^n} A$ означает, что элемент $a_{(n)}$ и множество $A_{(n)}$ находятся в отношении $*$ $\in \{\in, \notin\}$, $a \in \mathbb{Z}$, $A \subset \mathbb{Z}$; запись $B *_{2^n} C$ означает, что множества $B_{(n)}$ и $C_{(n)}$ находятся в отношении $*$ $\in \{\subseteq, \not\subseteq, =, \equiv\}$, $B, C \subset \mathbb{Z}$ и (B, C) могут быть одноэлементными множествами; $\alpha * B = \{\alpha * \beta \mid \beta \in B\}$ для подмножества B и элемента α группы $X \in \{\mathbb{Z}_{2^n}^+, V_n^+\}$ с бинарной операцией $*$ $\in \{+, \oplus\}$; $\varphi_i^{(R)}$ – естественный гомоморфизм подгруппы R импримитивной группы P_n в группу, действующую на множестве $W^{(i,n)} = \{W_0^{(i,n)}, \dots, W_{2^i-1}^{(i,n)}\}$ блоков импримитивности i -й системы импримитивности, определяемой группой $\mathbb{Z}_{2^n}^+$, т.е. $W_t^{(i,n)} = \{j \in \mathbb{Z}_{2^n} \mid j \equiv_{2^i} t\}$, $i = 1, \dots, n-1$; $\text{Кег } \varphi_0^{(R)} = R$ для $R \leq P_n$; $\varepsilon_{j,n} = (0, \dots, 0, 1, \underbrace{0, \dots, 0}_{j-1})$, $\|\alpha\|$ – логарифмическая норма [1]

элемента $\alpha \in \mathbb{Z}_{2^n}$, т.е. $\alpha = 2^{\|\alpha\|} \beta$, $2 \nmid \beta$; $J_B(f)$ – группа инерции функции $f \in F_{n,m}^*$ относительно группы $B \leq S(X_n^*)$, $*$ $\in \{\oplus, +\}$; $X =_{2^n} Y$, если $X = Y_{(n)}$, $Y, X \subseteq \mathbb{Z}_{2^n}$; $\alpha =_{2^n} \beta$, если $\alpha = \beta_{(n)}$ для $\alpha, \beta \in \mathbb{Z}_{2^n}$;

$$\sum_{\alpha \in W} * = \begin{cases} \sum_{\alpha \in W} \oplus = \bigoplus_{\alpha \in W} \alpha, & \text{если } * = \oplus, \\ \sum_{\alpha \in W} 2^m, & \text{если } * \text{ – операция } + \text{ сложения в кольце } \mathbb{Z}_{2^m}; \end{cases}$$

$$X_n^* = \begin{cases} V_n, & \text{если } * = \oplus, \\ \mathbb{Z}_{2^n}, & \text{если } * = +, \end{cases} \quad \Delta_H^* = \begin{cases} \Delta_H^+, & \text{если } * = +, \\ \Delta_H^\oplus, & \text{если } * = \oplus. \end{cases}$$

Всюду ниже предполагается, что $n, m \in \mathbb{N}$, $m \leq n$, $n \geq 2$.

Пусть X, Y – конечные абелевы группы, H – подгруппа симметрической группы $S(X)$.

Определение 2.1. Орбитальной производной отображения $f: X \rightarrow Y$ по группе H или H -производной называется оператор Δ_H , задаваемый формулой

$$\Delta_H f(x) = \sum_{\beta \in x^H} f(\beta).$$

Если $H = \langle a \rangle$, то H -производную также будем называть производной по элементу $a \in H$.

Пусть $n, m \in \mathbb{N}$, $m \leq n$. Для $X = \mathbb{Z}_{2^n}^+$, $Y = \mathbb{Z}_{2^m}^+$ G^+ -производной называется оператор

$$\Delta_G^+ : f(x) \mapsto \sum_{\alpha \in x^G} f(\alpha) \pmod{2^n},$$

а для $X = V_n^+$, $Y = V_m^+ G^\oplus$ -производной – оператор

$$\Delta_G^\oplus : f(x) \mapsto \bigoplus_{\alpha \in xG} f(\alpha).$$

Если δ_β – сдвиг на вектор $\beta \in V_n$, т.е. $\delta_\beta : x \mapsto x \oplus \beta$, то $\{\{\lambda, \lambda \oplus \beta\} | \lambda \in V_n\}$ – множество всех орбит подгруппы $\langle \delta_\beta \rangle$ и $\langle \delta_\beta \rangle_\oplus$ -производная функции $f \in F_{n,m}^\oplus$, определяемая условием $\Delta_{\langle \delta_\beta \rangle}^\oplus f : x \mapsto f(x) \oplus f(x \oplus \beta)$, т.е. совпадает с традиционным определением производной по направлению вектора β (см., например, [2]).

Положим $h_n = (0, 1, 2, \dots, 2^n - 1)$. Так как для $t \in \{1, \dots, n - 1\}$ орбита группы $G = \langle h_n^{2^t} \rangle$, содержащая элемент $\alpha \in \mathbb{Z}_{2^n}$, равна

$$\left\{ (\alpha + 2^t c)_{(n)} | c \in \{0, \dots, 2^{n-t} - 1\} \right\},$$

то G^+ -производная отображения $f \in F_{n,m}^+$ задаётся оператором Δ_G^+ , где

$$\Delta_G^+ f(x) = \sum_{\beta \in \langle 2^t \rangle} f(x + \beta),$$

и совпадает с определением $(n - t)$ -й орбитальной производной [3].

Для отображения $f \in F_{n,m}^\oplus$ традиционное определение высшей производной по линейно независимым векторам $\beta_1, \dots, \beta_r \in V_n$ есть

$$\Delta_{\langle \delta_{\beta_1} \rangle}^\oplus \dots \Delta_{\langle \delta_{\beta_r} \rangle}^\oplus f(x) = \bigoplus_{\alpha \in x \langle \delta_{\beta_1}, \dots, \delta_{\beta_r} \rangle} f(\alpha). \quad (2.1)$$

Легко видеть, что для групп $H_1, \dots, H_r \leq S(X)$ выполняются равенства

$$\begin{aligned} \Delta_{H_2}(\Delta_{H_1} f(x)) &= \Delta_{H_2} \left(\sum_{\beta \in x^{H_1}} f(\beta) \right) = \sum_{\beta \in x^{H_1}} \Delta_{H_2} f(\beta) = \\ &= \sum_{\beta \in x^{H_1}} \sum_{\alpha \in \beta^{H_2}} f(\alpha). \end{aligned} \quad (2.2)$$

Поэтому естественным обобщением орбитальной производной будет

$$\Delta_{H_1, \dots, H_r} f(x) = \sum_{\beta \in x^{H_1 H_2 \dots H_r}} f(\beta). \quad (2.3)$$

В частности, для групп $H_1 = \langle \delta_{\beta_1} \rangle, \dots, H_r = \langle \delta_{\beta_r} \rangle$ имеем

$$\Delta_{H_1, \dots, H_r}^\oplus f(x) = \Delta_{H_r}^\oplus \dots \Delta_{H_1}^\oplus f(x).$$

Более того, если подгруппы $H_1, \dots, H_r$ группы $H \leq S(X)$ перестановочны (например, они нормальны в H), то

$$\Delta_{H_1, \dots, H_r} f(x) = \sum_{\beta \in x^{H_1 \dots H_r}} f(\beta) = \sum_{\beta \in x^{\langle H_1, H_2, \dots, H_r \rangle}} f(\beta).$$

Определение 2.2. Отображение $f : X \rightarrow Y$ назовём *константным*, если $f(x) = c$ для некоторого элемента $c \in Y$ при всех $x \in X$.

Пусть $O(G)$ – множество всех орбит неединичной длины группы $G \leq S(V_n)$, $\overline{O}(G)$ – множество всех нетривиальных орбит всех подгрупп группы G , т.е. $\overline{O}(G) = \bigcup_{B \leq G} O(B)$.

3. Свойства оператора взятия производной

Всюду в данном разделе $*$ $\in \{\oplus, +\}$.

Для $j = 0, \dots, n$ положим

$$F_{n,m}^{+(j)} = \{f \in F_{n,m}^+ | f(\alpha) = f(\alpha + c \cdot 2^j) \forall (\alpha, c) \in \{0, \dots, 2^j - 1\} \times \{0, \dots, 2^{n-j} - 1\}\},$$

$$F_{n,m}^{\oplus(j)} = \{f \in F_{n,m}^{\oplus} | f(\alpha) = f(\alpha \oplus \delta) \forall (\alpha, \delta) \in \langle \varepsilon_{0,n}, \dots, \varepsilon_{j-1,n} \rangle \times \langle \varepsilon_{j,n}, \dots, \varepsilon_{n-1,n} \rangle\},$$

$$\overline{F}_{n,m}^{*(0)} = F_{n,m}^{*(0)}, \quad \overline{F}_{n,m}^{*(j)} = F_{n,m}^{*(j)} \setminus F_{n,m}^{*(j-1)}.$$

В дискретной математике при рассмотрении производных отображения $f : X \rightarrow Y$ по элементам $\beta_2, \beta_1 \in X$ полагают

$$\Delta_{\beta_2} \Delta_{\beta_1} f(x) = \Delta_{\beta_2} (\Delta_{\beta_1} f(x)), \quad (3.1)$$

где $(X, Y) \in \{(\mathbb{Z}_{2^n}, \mathbb{Z}_{2^m}), (V_n, V_m)\}$ и элемент $\beta \in X$ удовлетворяет равенству

$$\Delta_{\beta} f(x) = \begin{cases} f(x) \oplus f(x \oplus \beta), & \text{если } f \in F_{n,m}^{\oplus}, \\ f(x + \beta) - f(x), & \text{если } f \in F_{n,m}^+. \end{cases}$$

Для групп $H_1, H_2 \leq S(X)$ и орбитальных производных равенство (3.1) принимает вид

$$\Delta_{H_2} \Delta_{H_1} f(x) = \Delta_{H_2} (\Delta_{H_1} f(x)) = \sum_{\gamma_1 \in x^{H_2}} \sum_{\gamma_2 \in \gamma_1^{H_1}} f(\gamma_2).$$

Пусть $\deg f$ – алгебраическая степень двоичной функции $f \in F_{n,1}^{\oplus}$. Известно, что для $t \geq \deg f + 1$, произвольных векторов $\beta_1, \dots, \beta_t \in V_n^{\times}$ выполняется равенство $\Delta_{\beta_t} \dots \Delta_{\beta_1} f(x) = 0$. Однако описание свойств производных для отображений из $F_{n,m}^+$ сложнее. В [8] показано, что при $t \geq 2^{n-1}(m+1) - 1$ выполняется равенство $\Delta_{\beta_t} \dots \Delta_{\beta_1} f(x) = 0$ для произвольного отображения $f \in F_{n,m}^+$ и произвольных элементов $\beta_1, \dots, \beta_t \in \mathbb{Z}_{2^n}^{\times}$. Получение аналогичных результатов для орбитальных производных по произвольной абелевой группе или подгруппе группы P_n существенно сложнее.

Пусть $\text{ord}(b)$ – порядок элемента b в $S(\mathbb{Z}_{2^n})$.

Утверждение 3.1. Пусть $n \geq 2$, $\alpha \in \mathbb{Z}_{2^n}$, G – абелева подгруппа группы $S(\mathbb{Z}_{2^n})$, $|G| = 2^r$ для некоторого числа $r \in \mathbb{N}$. Тогда для произвольного отображения $f \in F_{n,m}^+$ существует такое число $l \in \mathbb{N}$, что для любой последовательности $(a_1, \dots, a_l) \in G^l$ со свойством $|\alpha^{(a_i)}| \geq 2$, $i = 1, \dots, l$, выполняется равенство $\Delta_{\langle a_l \rangle}^+ \left(\Delta_{\langle a_{l-1} \rangle}^+ \left(\dots \left(\Delta_{\langle a_1 \rangle}^+ f(\alpha) \right) \right) \right) = 2^m 0$.

Доказательство. Пусть $b_1, \dots, b_c$ – произвольные элементы группы G . Очевидно, что $\Delta_{\langle b_i \rangle}^+ \Delta_{\langle b_j \rangle}^+ f(\alpha) = {}_{2^m} \Delta_{\langle b_j \rangle}^+ \Delta_{\langle b_i \rangle}^+ f(\alpha)$ для $i, j \in \{1, \dots, c\}$. Отметим, что

$$\Delta_{\langle b_c \rangle}^+ \dots \Delta_{\langle b_1 \rangle}^+ f(\alpha) = {}_{2^m} \Delta_{\langle b_c \rangle}^+ \dots \Delta_{\langle b_1 \rangle}^+ f(\delta) \quad (3.2)$$

для произвольного элемента $\delta = \alpha^{b_1^{t_1} \dots b_c^{t_c}} \in \alpha^{\langle b_1 \rangle \dots \langle b_c \rangle}$, так как при некоторых $t_j \in \{0, \dots, \text{ord}(b_j) - 1\}$, $j = 1, \dots, c$,

$$\begin{aligned} \Delta_{\langle b_c \rangle}^+ \dots \Delta_{\langle b_1 \rangle}^+ f(\delta) &= {}_{2^m} \Delta_{\langle b_c \rangle}^+ \dots \Delta_{\langle b_1 \rangle}^+ f(\alpha^{b_1^{t_1} \dots b_c^{t_c}}) = {}_{2^m} \\ &= {}_{2^m} \sum_{i_1=0}^{\text{ord}(b_1)-1} \dots \sum_{i_c=0}^{\text{ord}(b_c)-1} f\left(\alpha^{b_1^{t_1} \dots b_c^{t_c} b_1^{i_1} \dots b_c^{i_c}}\right) = {}_{2^m} \\ &= {}_{2^m} \sum_{i_1=0}^{\text{ord}(b_1)-1} \dots \sum_{i_c=0}^{\text{ord}(b_c)-1} f\left(\alpha^{b_1^{t_1+i_1} \dots b_c^{t_c+i_c}}\right) = {}_{2^m} \Delta_{\langle b_c \rangle}^+ \dots \Delta_{\langle b_1 \rangle}^+ f(\alpha). \end{aligned}$$

Из равенства (3.2) следует существование такого отображения $f' \in F_{n,m}^+$, что справедливо равенство

$$\Delta_{\langle b_c \rangle}^+ \dots \Delta_{\langle b_1 \rangle}^+ f(\alpha) = {}_{2^m} \sum_{\beta \in \alpha^{\langle b_1, \dots, b_c \rangle}} f'(\beta).$$

Пусть $p, r \in \mathbb{N}$. Если $b_{c+1}, \dots, b_{c+p} \in \langle b_1, \dots, b_c \rangle \setminus \{e\}$, то

$$\begin{aligned} \Delta_{\langle b_{c+p} \rangle}^+ \dots \Delta_{\langle b_{c+1} \rangle}^+ \Delta_{\langle b_c \rangle}^+ \dots \Delta_{\langle b_1 \rangle}^+ f(\alpha) &= {}_{2^m} \Delta_{\langle b_{c+p} \rangle}^+ \dots \Delta_{\langle b_{c+1} \rangle}^+ \sum_{\beta \in \alpha^{\langle b_1, \dots, b_c \rangle}} f'(\beta) = {}_{2^m} \\ &= {}_{2^m} \left| \alpha^{\langle b_{c+1} \rangle} \right| \cdot \dots \cdot \left| \alpha^{\langle b_{c+p} \rangle} \right| \sum_{\beta \in \alpha^{\langle b_1, \dots, b_c \rangle}} f'(\beta). \end{aligned} \quad (3.3)$$

Так как $|G| = 2^r$, то число $|\langle b_t \rangle|$ чётно, $|\alpha^{\langle b_t \rangle}| \geq 2$, для $t \in \{1, \dots, p\}$ и для $p = m$ имеем

$$\Delta_{\langle b_{c+p} \rangle}^+ \dots \Delta_{\langle b_{c+1} \rangle}^+ \Delta_{\langle b_c \rangle}^+ \dots \Delta_{\langle b_1 \rangle}^+ f(\alpha) = {}_{2^p} 0. \quad (3.4)$$

Для произвольных элементов $s_1, \dots, s_r \in G$ положим

$$u(s_1, \dots, s_r) = \sum_{j=2}^r I(s_j \in \langle s_1, \dots, s_{j-1} \rangle),$$

где $I(B)$ – индикатор выполнения условия B .

Индукцией по r , используя соотношения (3.3) и (3.4), нетрудно показать, что

$$\Delta_{\langle s_r \rangle}^+ \dots \Delta_{\langle s_1 \rangle}^+ f(x) \equiv 0 \pmod{2^{u(s_1, \dots, s_r)}}.$$

Нетрудно убедиться, что для $l \geq m|G|$ и произвольных элементов $(a_1, \dots, a_l) \in G^l$ выполняется соотношение $u(a_1, \dots, a_l) \geq m$. Таким образом,

$$\Delta_{\langle a_l \rangle}^+ \dots \Delta_{\langle a_1 \rangle}^+ f(x) = {}_{2^m} 0.$$

Утверждение доказано.

Аналогично утверждению 4.1 [5] показывается, что для произвольных отображения $f \in F_{n,m}^\oplus$, абелевой группы $G \leq S(V_n)$ чётного порядка и такого набора $(a_1, \dots, a_l) \in G^l$, что $|\alpha^{(a_i)}| \geq 2$ для $i = 1, \dots, l$ и $l \geq 2|G|$, выполняется равенство

$$\Delta_{\langle a_l \rangle}^\oplus \left(\Delta_{\langle a_{l-1} \rangle}^\oplus \left(\dots \left(\Delta_{\langle a_1 \rangle}^\oplus f(\alpha) \right) \right) \right) = 0.$$

Приведём свойства орбитальной производной.

Лемма 3.1. Пусть $n \geq 2$, $R \in \{G_n, P_n\}$, $* \in \{+, \oplus\}$, $f \in F_{n,m}^*$, $i \in \{1, \dots, n\}$. Тогда:

- 1) $\Delta_{\text{Ker } \varphi_{n-i}^{(R)}}^* f(x) \in F_{n,m}^{*(n-i)}$,
- 2) для каждой $\theta \in X_n^*$, $b \in R$:
 - а) $\Delta_{\langle b \rangle}^* f(\alpha) = \Delta_{\langle b \rangle}^* f(\beta)$ для любых $\alpha, \beta \in \theta^{(b)}$,
 - б) $|\theta^{(b)}|$ чётно, если $b \neq e$.

Доказательство. Доказательство очевидно.

Для элементов $b_1, b_2 \in P_n \setminus \{e\}$ приведём свойства оператора $\Delta_{\langle b_2 \rangle}^+ \left(\Delta_{\langle b_1 \rangle}^+ \right)$.

Утверждение 3.2. Пусть $n \geq 2$, $* \in \{+, \oplus\}$, $t \in \{1, \dots, n-1\}$, $b_1, b_2 \in P_n \setminus \{e\}$, $\alpha \in X_n^*$. Тогда:

- 1) Если $x^{(b_1)} = x^{(b_2)}$, то

$$\Delta_{\langle b_2 \rangle}^+ \left(\Delta_{\langle b_1 \rangle}^+ f(x) \right) = \Delta_{\langle b_1 \rangle}^+ \left(\Delta_{\langle b_2 \rangle}^+ f(x) \right) =_{2^m} |x^{(b_1)}| \cdot \Delta_{\langle b_2 \rangle}^+ f(x),$$

$$\Delta_{\langle b_2 \rangle}^\oplus \left(\Delta_{\langle b_1 \rangle}^\oplus f(x) \right) = 0.$$

- 2) Если $\alpha^{(b_i)} = \alpha \oplus \left\langle \varepsilon_{p_i^{(i)}, n}, \dots, \varepsilon_{p_{r_i}^{(i)}, n} \right\rangle$ для некоторых $r_i < n$, $0 \leq p_1^{(i)} < \dots < p_{r_i}^{(i)} \leq n-1$, $i \in \{1, 2\}$, то

$$\begin{aligned} \alpha^{\langle b_1 \rangle \langle b_2 \rangle} &= \alpha^{\langle b_2 \rangle \langle b_1 \rangle} = \alpha^{\langle b_1, b_2 \rangle} = \\ &= \alpha \oplus \left\langle \varepsilon_{p_1^{(1)}, n}, \dots, \varepsilon_{p_{r_1}^{(1)}, n} \right\rangle \oplus \left\langle \varepsilon_{p_1^{(2)}, n}, \dots, \varepsilon_{p_{r_2}^{(2)}, n} \right\rangle. \end{aligned}$$

- 3) Если $\alpha^{\langle b_1 \rangle} \cap \alpha^{\langle b_2 \rangle} = \{\alpha\}$, то

$$\Delta_{\langle b_2 \rangle}^* \left(\Delta_{\langle b_1 \rangle}^* f(\alpha) \right) = \Delta_{\langle b_1 \rangle}^* \left(\Delta_{\langle b_2 \rangle}^* f(\alpha) \right) = \Delta_{\langle b_1, b_2 \rangle}^* f(\alpha).$$

- 4) Если $\alpha^{(b_i)} = \alpha \oplus \left\langle \varepsilon_{p_i^{(i)}, n}, \dots, \varepsilon_{p_{r_i}^{(i)}, n} \right\rangle$ для $i = 1, 2$ и

$$c = \dim \left(\left\langle \varepsilon_{p_1^{(1)}, n}, \dots, \varepsilon_{p_{r_1}^{(1)}, n} \right\rangle \cap \left\langle \varepsilon_{p_1^{(2)}, n}, \dots, \varepsilon_{p_{r_2}^{(2)}, n} \right\rangle \right),$$

то

$$\Delta_{\langle b_2 \rangle}^* \left(\Delta_{\langle b_1 \rangle}^* f(\alpha) \right) = 2^c \left(\Delta_{\langle b_1, b_2 \rangle}^* f(\alpha) \right).$$

Доказательство. 1) Применяя п. 2 леммы 3.1, получаем

$$\Delta_{\langle b_2 \rangle}^+ \left(\Delta_{\langle b_1 \rangle}^+ f(x) \right) =_{2^m} \sum_{\beta \in x^{\langle b_2 \rangle}} \Delta_{\langle b_1 \rangle}^+ f(\beta) =_{2^m} |x^{\langle b_1 \rangle}| \Delta_{\langle b_1 \rangle}^+ f(x),$$

$$\Delta_{\oplus}^{\langle b_2 \rangle} \left(\Delta_{\oplus}^{\langle b_1 \rangle} f(x) \right) = |x^{\langle b_2 \rangle}| \Delta_{\oplus}^{\langle b_1 \rangle} f(x) = 0.$$

Для операции $*$ $\in \{+, \oplus\}$ равенство $\Delta_{\langle b_2 \rangle}^* \left(\Delta_{\langle b_1 \rangle}^* f(x) \right) = \Delta_{\langle b_1 \rangle}^* \left(\Delta_{\langle b_2 \rangle}^* f(x) \right)$ очевидно.

2) Нетрудно убедиться, что орбита произвольного элемента $\alpha \in \mathbb{Z}_{2^n}$ в группе $H < P_n$ имеет вид

$$\alpha^H = \alpha \oplus \{ \varepsilon_{p_1, n} u_1 \oplus \dots \oplus \varepsilon_{p_r, n} u_r | u_1, \dots, u_r \in \{0, 1\} \}$$

для некоторых чисел $p_1, \dots, p_r \in \{0, \dots, n-1\}$, $0 \leq p_1 < p_2 < \dots < p_r$, $r < n$.

Поэтому предположим, что орбита элемента $\alpha \in \mathbb{Z}_{2^n}$ в группе $\langle b_i \rangle$ есть

$$\alpha^{\langle b_i \rangle} = \alpha \oplus \left\{ \varepsilon_{p_1^{(i)}, n} u_1 \oplus \dots \oplus \varepsilon_{p_{r_i}^{(i)}, n} u_{r_i} | u_1, \dots, u_{r_i} \in \{0, 1\} \right\},$$

где $\{p_1^{(i)}, \dots, p_{r_i}^{(i)}\} \subseteq \{0, \dots, n-1\}$, $0 \leq p_1^{(i)} < \dots < p_{r_i}^{(i)} \leq n-1$, $r_i < n$, $i \in \{1, 2\}$.

Согласно утверждению 3.3 [5] множество всех орбит группы $\langle b_i \rangle$ на множестве $\alpha \oplus \langle \varepsilon_{p_1^{(i)}, n}, \varepsilon_{p_1^{(i)}+1, n}, \dots, \varepsilon_{n-1, n} \rangle$ равно

$$\left\{ \beta \oplus \langle \varepsilon_{p_1^{(i)}, n}, \dots, \varepsilon_{p_{r_i}^{(i)}, n} \rangle \mid \beta \in \alpha \oplus \langle \varepsilon_{p_1^{(i)}, n}, \varepsilon_{p_1^{(i)}+1, n}, \dots, \varepsilon_{n-1, n} \rangle \right\}.$$

Значит,

$$\alpha^{\langle b_1 \rangle \langle b_2 \rangle} = \alpha^{\langle b_2 \rangle \langle b_1 \rangle} = \alpha \oplus \langle \varepsilon_{p_1^{(1)}, n}, \dots, \varepsilon_{p_{r_1}^{(1)}, n} \rangle \oplus \langle \varepsilon_{p_1^{(2)}, n}, \dots, \varepsilon_{p_{r_2}^{(2)}, n} \rangle.$$

П. 3) следует из п. 2), а п. 4) следует из пп. 2), 3) и того, что в мультимножестве $\left\{ \left\{ \langle \varepsilon_{p_1^{(1)}, n}, \dots, \varepsilon_{p_{r_1}^{(1)}, n} \rangle \oplus \langle \varepsilon_{p_1^{(2)}, n}, \dots, \varepsilon_{p_{r_2}^{(2)}, n} \rangle \right\} \right\}$ каждый вектор из векторного пространства $\langle \varepsilon_{p_1^{(1)}, n}, \dots, \varepsilon_{p_{r_1}^{(1)}, n}, \varepsilon_{p_1^{(2)}, n}, \dots, \varepsilon_{p_{r_2}^{(2)}, n} \rangle$ встречается ровно 2^c раз, при этом $\alpha^{\langle b_1, b_2 \rangle} = \langle \varepsilon_{p_1^{(1)}, n}, \dots, \varepsilon_{p_{r_1}^{(1)}, n}, \varepsilon_{p_1^{(2)}, n}, \dots, \varepsilon_{p_{r_2}^{(2)}, n} \rangle$.

Лемма доказана.

Для группы $H \leq P_n$ и функции $f \in F_{n, m}^*$ опишем свойства группы инерции $J_{S(X_n^*)}(\Delta_H^* f)$.

Пусть $N_{S(X_n^*)}(H)$ – нормализатор группы H в группе $S(X_n^*)$, $H \leq S(X_n^*)$.

Утверждение 3.3. Пусть $n \geq 2$ и $*$ $\in \{\oplus, +\}$, $f \in F_{n, m}^*$, $H, H' \leq P_n$.

1) Если $H, H' \leq J_{S(X_n^*)}(f)$, то

$$\Delta_H^* f(x) = |x^H| f(x), \quad \Delta_{H'}^* (\Delta_H^* f(x)) = |x^H| \cdot |x^{H'}| f(x).$$

2) $\langle H, J_{S(X_n^*)}(f) \cap N_{S(X_n^*)}(H) \rangle \subseteq J_{S(X_n^*)}(\Delta_H^* f)$.

3) $J_{S(X_n^*)} \left(\Delta_{\text{Ker } \varphi_{n-i}^{(B)}}^* f \right) \leq J_{S(X_n^*)} \left(\Delta_{\text{Ker } \varphi_{n-i-1}^{(B)}}^* f \right)$ для $i \in \{0, \dots, n-1\}$.

Доказательство. 1) Указанные соотношения следуют из того, что для каждого $g \in J_{S(X_n^*)}(f)$ справедливо равенство $f(x) = f(x^g)$.

2) Включение $H \leq J_{S(X_n^*)}(\Delta_H^* f)$ следует из того, что для каждого $g \in H$ выполняется равенство

$$\Delta_H^* f(x^g) = \sum_{\beta \in x^g H} {}^* f(\beta) = \sum_{\beta \in x^H} {}^* f(\beta) = \Delta_H^* f(x).$$

Для элемента $\alpha \in V_n$ обозначим через $R_H(\alpha)$ такое подмножество наименьшей мощности группы H , что $\alpha^H = \alpha^{R_H(\alpha)}$. Ясно, что $|R_H(\alpha)| = |\alpha^H|$. Тогда для каждого $g \in J_{S(X_n^*)}(f) \cap N_{S(X_n^*)}(H)$

$$\begin{aligned} \Delta_H^* f(x^g) &= \sum_{\beta \in x^g H} {}^* f(\beta) = \sum_{\beta \in x^H g} {}^* f(\beta) = \\ &= \sum_{r \in R_H(\alpha)} {}^* f(x^{rg}) = \sum_{r \in R_H(\alpha)} {}^* f(x^r) = \Delta_H^* f(x). \end{aligned}$$

Значит, $J_{S(X_n^*)}(f) \cap N_{S(X_n^*)}(H) \subseteq J_{S(X_n^*)}(\Delta_H^* f)$. Таким образом,

$$\langle H, J_{S(X_n^*)}(f) \cap N_{S(X_n^*)}(H) \rangle \subseteq J_{S(X_n^*)}(\Delta_H^* f).$$

3) Включения следуют из строения множества орбит групп $\text{Ker } \varphi_{n-i}^{(B)}$, $\text{Ker } \varphi_{n-i-1}^{(B)}$. Утверждение доказано.

Приведём пример невыполнения равенства

$$\langle H, J_{S(X_n^*)}(f) \cap N_{S(X_n^*)}(H) \rangle = J_{S(X_n^*)}(\Delta_H^* f).$$

Пример 3.1. Пусть $B \in \{G_n, P_n\}$, $m = n$, $c \in \{1, \dots, 2^{n-1} - 1\}$, s – произвольная подстановка из $S(\{0, \dots, 2^{n-1} - 1\})$ и отображение $f \in S(\mathbb{Z}_{2^n})$ задано условием

$$f : i \mapsto \begin{cases} i^s, & \text{если } i \in \{0, \dots, 2^{n-1} - 1\}, \\ \left(c - (i - 2^{n-1})^s \right)_{(n)}, & \text{если } i \in \{2^{n-1}, \dots, 2^n - 1\}. \end{cases}$$

Очевидно, что

$$f(x) + f(x + 2^{n-1}) = {}_{2^n}c, \quad J_{S(X_n^+)}(f) = \langle e \rangle.$$

Тогда $\langle H, J_{S(X_n^+)}(f) \rangle = \text{Ker } \varphi_{n-1}^{(B)}$, а $J_{S(X_n^+)} \left(\Delta_{\text{Ker } \varphi_{n-1}^{(B)}}^+ f \right) = S(\mathbb{Z}_{2^n})$. Таким образом,

$$\langle H, J_{S(X_n^+)}(f) \rangle < J_{S(X_n^+)}(\Delta_H^+ f).$$

Аналогичный пример можно привести при $m < n$.

Пусть $\wr$ – операция сплетения групп подстановок.

Из утверждения 3.3 и примера 3.1 следует, что при $B \in \{G_n, P_n\}$ существуют такие функции $f \in F_{n,m}^*$ и ряд подгрупп $\bar{H} = (\langle e \rangle, H_1, \dots, H_{l-1}, B)$, где $H_i < B$ и $H_i < H_{i+1}$ при $i = 1, \dots, l - 2$, что:

- 1) $J_{S(X_n^*)}(\Delta_B^* f) = S(X_n^*)$;
- 2) $J_{S(X_n^*)} \left(\Delta_{\text{Ker } \varphi_{n-i}^{(B)}}^* f \right) \geq S_{2^i} \wr S_{2^{n-i}}$, если $\text{Ker } \varphi_{n-i}^{(B)} \in \{H_1, \dots, H_{l-1}\}$ при $i \in \{1, \dots, l-2\}$;
- 3) $J_{S(X_n^*)}(\Delta_{H_i}^* f) \geq J_{S(X_n^*)}(\Delta_{H_{i+1}}^* f) \leq J_{S(X_n^*)}(\Delta_{H_{i+2}}^* f)$ для некоторых $i \in \{2, \dots, l-3\}$, причём первое и второе неравенства могут быть строгими.

4. Неуплотняемые последовательности орбит групп G_n , P_n и степень асимметричности 1-го типа

Пусть $U^{(1)}, U^{(2)}$ – два различных подмножества множества орбит подгрупп H_1, H_2 группы $S(\mathbb{Z}_{2^n})$. Будем считать, что $U^{(1)} \prec U^{(2)}$, если $U^{(1)} \neq U^{(2)}$ и для каждой орбиты $\Lambda \in U^{(1)}$ существует такая орбита $\Lambda' \in U^{(2)}$, что $\Lambda \subseteq \Lambda'$, т.е. элементы множества $U^{(2)}$ являются объединением некоторых орбит из множества $U^{(1)}$. Пусть $E_n = \{\{j\} | j \in \{0, \dots, 2^n - 1\}\}$ – множество орбит группы $\langle e \rangle$.

Назовём последовательность $\bar{U} = (U^{(1)}, \dots, U^{(l)})$ длины l , элементы которой принадлежат множеству $\bar{O}(B)$, (B, l) -последовательностью, если

$$U^{(1)} \prec U^{(2)} \prec \dots \prec U^{(l-1)} \prec U^{(l)}. \quad (4.1)$$

В случае, когда длина последовательности $\bar{U}$ неизвестна или её конкретное значение несущественно, число l будем опускать и (B, l) -последовательность называть B -последовательностью. Ряд подгрупп (4.1) позволяет классифицировать отображения по свойствам их групп инерции.

Назовём B -последовательность $\bar{U} = (U^{(1)}, \dots, U^{(l)})$ *плотной*, если для каждого $j \in \{2, \dots, l\}$ не существует такого множества $\tilde{U}^{(j)} \in \bar{O}(B)$, что $U^{(j-1)} \prec \tilde{U}^{(j)} \prec U^{(j)}$. Пусть $\bar{U}(B) = \{U^{(1)}, \dots, U^{(l)}\}$ – множество всех элементов последовательности $\bar{U}$.

Очевидно, что каждой B -последовательности соответствует такой ряд подгрупп

$$H^{(1)} < H^{(2)} < \dots < H^{(l-1)} < H^{(l)} \quad (4.2)$$

группы B , $H^{(l)} \leq B$, что $U^{(i)}$ – множество орбит подгруппы $H^{(i)}$, $i = 1, \dots, l$. Плотную последовательность $E_n \prec \dots \prec O(B)$ назовём *неуплотняемой B -последовательностью*.

Опишем неуплотняемые P_n - и G_n -последовательности.

Утверждение 4.1. 1) Пусть $n \geq 2$, $D_{t_i}^{(i)} \subseteq \{0, \dots, 2^{n-i} - 1\}$, $|D_{t_i}^{(i)}| = t_i$, причём

$$D_1^{(i)} \prec D_2^{(i)} \prec \dots \prec D_{2^{n-i}}^{(i)}$$

и $X_{t_i}^{(i)} = \{0, \dots, 2^{n-i+1} - 1\} \setminus \bigcup_{j \in D_{t_i}^{(i)}} \{j, j + 2^{n-i}\}$, $t_i = 1, 2, \dots, 2^{n-i}$, $i = 1, 2, \dots, n-1$.

Пусть также

$$U_{t_1}^{(1)} = \left\{ r \oplus \langle \varepsilon_{n-1, n} \rangle \mid r \in D_{t_1}^{(1)} \right\}, \quad t_1 = 1, \dots, 2^{n-1},$$

$$U_{t_i}^{(i)} = \left\{ r \oplus \langle \varepsilon_{n-i,n}, \dots, \varepsilon_{n-1,n} \rangle \mid r \in D_{t_i}^{(i)} \right\} \bigcup \left\{ r' \oplus \langle \varepsilon_{n-i+1,n}, \dots, \varepsilon_{n-1,n} \rangle \mid r' \in X_{t_i}^{(i)} \right\},$$

где $t_i = 1, \dots, 2^{n-i}$, $i = 2, \dots, n-1$. Тогда последовательность

$$\left(E, U_1^{(1)}, \dots, U_{2^{n-1}}^{(1)}, U_1^{(2)}, \dots, U_{2^{n-2}}^{(2)}, \dots, U_1^{(n-2)}, U_2^{(n-2)}, \right. \\ \left. U_3^{(n-2)}, U_4^{(n-2)}, U_1^{(n-1)}, U_2^{(n-1)}, \{0, \dots, 2^n - 1\} \right) \quad (4.3)$$

является неуплотняемой P_n -последовательностью длины 2^n .

2) Пусть $D_{t_i}^{(i)} \subseteq \{0, \dots, 2^{n-i-1} - 1\}$, $|D_{t_i}^{(i)}| = t_i$, причём

$$D_1^{(i)} \prec D_2^{(i)} \prec \dots \prec D_{2^{n-i-1}}^{(i)},$$

$$\text{и } X_{t_i}^{(i)} = \{0, \dots, 2^{n-i} - 1\} \setminus \bigcup_{j \in D_{t_i}^{(i)}} \{j, j + 2^{n-i-1}\}, \quad t_i = 1, 2, \dots, 2^{n-i}, \quad i = 1, 2, \dots, n-1.$$

Пусть также

$$U_{t_1}^{(1)} = \left\{ r \oplus \langle \varepsilon_{n-1,n} \rangle, r \oplus \langle \varepsilon_{n-1,n} \rangle \oplus \varepsilon_{n-2,n} \mid r \in D_{t_1}^{(1)} \right\}, \quad t_1 = 1, \dots, 2^{n-2},$$

$$U_{t_i}^{(i)} = \left\{ r \oplus \langle \varepsilon_{n-i,n}, \dots, \varepsilon_{n-1,n} \rangle, r \oplus \langle \varepsilon_{n-i,n}, \dots, \varepsilon_{n-1,n} \rangle \oplus \varepsilon_{n-i-1,n} \mid r \in D_{t_i}^{(i)} \right\} \bigcup$$

$$\bigcup \left\{ r' \oplus \langle \varepsilon_{n-i+1,n}, \dots, \varepsilon_{n-1,n} \rangle, r' \oplus \langle \varepsilon_{n-i+1,n}, \dots, \varepsilon_{n-1,n} \rangle \oplus \varepsilon_{n-i,n} \mid r' \in X_{t_i}^{(i)} \right\},$$

$$U_1^{(n-1)} = \{r \oplus \langle \varepsilon_{n-1,n}, \dots, \varepsilon_{1,n} \rangle \mid r \in \{0, 1\}\},$$

где $t_i = 1, \dots, 2^{n-i-1}$, $i = 2, \dots, n-1$. Тогда последовательность

$$\left(E, U_1^{(1)}, \dots, U_{2^{n-2}}^{(1)}, U_1^{(2)}, \dots, U_{2^{n-3}}^{(2)}, \dots, U_1^{(n-2)}, U_2^{(n-2)}, U_1^{(n-1)}, \{0, \dots, 2^n - 1\} \right) \quad (4.4)$$

является неуплотняемой G_n -последовательностью длины $2^{n-1} + 1$.

Доказательство следует из [5], точнее, из теоремы 3.1, утверждения 3.2 и следствия 3.4.

Заметим, что в п. 1) утверждения 3.1

$$U_{2^{n-i}}^{(i)} = \{r \oplus \langle \varepsilon_{n-i,n}, \dots, \varepsilon_{n-1,n} \rangle \mid r \in \{0, \dots, 2^{n-i-1} - 1\}\}$$

и $O(\text{Ker } \varphi_{n-i}^{(P_n)}) = U_{2^{n-i}}^{(i)}$, $i = 1, \dots, n-1$, согласно следствию 4.4. Из п. 2) утверждения 4.5 получаем, что $O(\text{Ker } \varphi_{n-i}^{(G_n)}) = U_{2^{n-i-1}}^{(i)}$.

Пусть $B \in \{G_n, P_n\}$, $\Omega(B)$ — множество всех неуплотняемых B -последовательностей, $\tilde{\Omega}(B)$ — множество всех неуплотняемых B -последовательностей, описанных в утверждении 4.1 (в п. 1 при $B = P_n$ и в п. 2 при $B = G_n$).

Покажем, что в утверждении 4.1 описаны все неуплотняемые B -последовательности, $B \in \{G_n, P_n\}$.

Следствие 4.1. Пусть $n \geq 2$. Справедливы равенства $\Omega(B) = \tilde{\Omega}(B)$ для $B \in \{G_n, P_n\}$.

Доказательство следует из теоремы 3.1, утверждения 3.2 и следствия 3.4 [5].

Таким образом, каждая неуплотняемая P_n -последовательность имеет длину 2^n , а неуплотняемая G_n -последовательность – длину $2^{n-1} + 1$.

Из утверждения 4.1 и следствия 4.1 следует, что если $B \in \{G_n, P_n\}$, $\bar{U}$ – произвольная неуплотняемая B -последовательность и C, C' – произвольные элементы последовательности $\bar{U}(B)$, $C \prec C'$, то её подпоследовательность $C \prec \dots \prec C'$ в $\bar{U}$ является плотной.

Пусть $B \in \{G_n, P_n\}$, $*$ $\in \{+, \oplus\}$. Обозначим через l_B длину неуплотняемой B -последовательности. Для отображения $f \in F_{n,m}^*$ и неуплотняемой B -последовательности $\bar{U} = (U_1, \dots, U_{l_B})$, $\bar{U} \in \Omega(B)$, соответствующей последовательности подгрупп $\bar{H} = (H_1, \dots, H_{l_B})$, обозначим через $d_B^{*(1)}(f, \bar{U})$ такое наименьшее число $c \in \{1, \dots, l_B\}$, что

$$\Delta_{H_{c-1}}^* (\dots \Delta_{H_2}^* (\Delta_{H_1}^* f(x))) \neq_{2^m} 0, \quad \Delta_{H_c}^* (\Delta_{H_{c-1}}^* (\dots \Delta_{H_2}^* (\Delta_{H_1}^* f(x)))) =_{2^m} 0.$$

Положим

$$d_{B,\min}^{*(1)}(f) = \min \left\{ d_B^{*(1)}(f, \bar{U}) \mid \bar{U} \in \Omega(B) \right\},$$

$$d_{B,\max}^{*(1)}(f) = \max \left\{ d_B^{*(1)}(f, \bar{U}) \mid \bar{U} \in \Omega(B) \right\}.$$

Величина $d_{B,\max}^{*(1)}(f)$ является аналогом понятия «степень нелинейности» для «классических производных», введённого в [8] для отображений над абелевыми группами. При этом рассматривается такая последовательность производных от функции f , что получившаяся функция является нулевой. В нашем случае возникают другие последовательности производных, подгруппами групп инерций которых являются элементы последовательности $\bar{H} = H_1, \dots, H_{l_B}$. Аналоги понятия «степень нелинейности» можно вводить и другими способами. Далее будут рассмотрены ещё два аналога понятия «степень нелинейности», обозначаемые $d_{B,\max}^{*(2)}(f)$, $d_{B,\max}^{*(3)}(f)$. Будем i -й аналог «степени нелинейности» называть степенью асимметрии i -го типа, $i = 1, 2, 3$.

Для $B \in \{G_n, P_n\}$, $*$ $\in \{+, \oplus\}$ положим

$$l_B^* = \begin{cases} 2^{n-2} + n, & (*, B) = (+, G_n), \\ 2^{n-2} + 1, & (*, B) = (\oplus, G_n), \\ 2^{n-1} + n, & (*, B) = (+, P_n), \\ 2^{n-1} + 1, & (*, B) = (\oplus, P_n). \end{cases}$$

Утверждение 4.2. Пусть $n \geq 2$, $B \in \{G_n, P_n\}$, $*$ $\in \{+, \oplus\}$, f – произвольное отображение из $F_{n,m}^*$, $\bar{U} \in \Omega(B)$. Тогда $d_B^{*(1)}(f, \bar{U}) \leq l_B^*$.

Доказательство. Приведём оценки величины $d_{G_n}^{+(1)}(f)$. Пусть

$$\left(\bar{U} = E, U_1^{(1)}, \dots, U_{2^{n-2}}^{(1)}, U_1^{(2)}, \dots, U_{2^{n-3}}^{(2)}, \dots, U_{n-2}^{(1)}, U_2^{(n-2)}, U_{n-1}^{(1)}, \{0, \dots, 2^n - 1\} \right),$$

$$H_i^{(j)} = O \left(U_j^{(i)} \right).$$

Зафиксируем набор $\left(q_1^{(1)}, \dots, q_{2^{n-2}}^{(1)} \right)$, $\left\{ q_1^{(1)}, \dots, q_{2^{n-2}}^{(1)} \right\} = \{0, \dots, 2^{n-2} - 1\}$ и рассмотрим последовательность подгрупп $\left(\bar{H}^{(1)} = \langle e \rangle, H_1^{(1)}, \dots, H_{2^{n-2}-1}^{(1)}, \text{Ker } \varphi_{n-1}^{(G_n)} \right)$, где $H_{2^{n-2}}^{(1)} = \text{Ker } \varphi_{n-1}^{(G_n)}$ и $H_j^{(1)} = \left\langle u_{q_1^{(1)}, n}, \dots, u_{q_j^{(1)}, n} \right\rangle$, $j = 1, \dots, 2^{n-2} - 1$. Последовательности $\bar{H}^{(1)}$ соответствует плотная G_n -последовательность $\bar{U}^{(1)} = \left(E_n, U_1^{(1)}, \dots, U_{2^{n-2}}^{(1)} \right)$ множеств орбит.

Несложно показать, что для $c = 1, \dots, 2^{n-2}$ справедливы равенства

$$\Delta_{H_c^{(1)}}^+ \left(\dots \Delta_{H_2^{(1)}}^+ \left(\Delta_{H_1^{(1)}}^+ f(\alpha) \right) \right) =_{2^n} \begin{cases} 2^c \left(f(\alpha) + f \left(\alpha u_{q_j^{(1)}, n} \right) \right), \\ \text{если } \exists j \in \{1, \dots, c\} : \left| \alpha \left\langle u_{q_j^{(1)}, n} \right\rangle \right| = 2, \\ f(\alpha), \text{ если } \left| \alpha \left\langle u_{q_j^{(1)}, n} \right\rangle \right| = 1 \forall j \in \{1, \dots, c\}. \end{cases} \quad (4.5)$$

Кроме того, если $\left| \alpha \left\langle u_{q_j^{(1)}, n} \right\rangle \right| = 2$ для $j \in \{1, \dots, 2^{n-2}\}$, то

$$\begin{aligned} f^{(1)}(\alpha) &=_{2^n} \Delta_{\text{Ker } \varphi_{n-1}^{(G_n)}}^+ \left(\Delta_{H_{2^{n-2}-1}^{(1)}}^+ \left(\dots \Delta_{H_2^{(1)}}^+ \left(\Delta_{H_1^{(1)}}^+ f(\alpha) \right) \right) \right) =_{2^n} \\ &=_{2^n} 2^{2^{n-2}-j} \left(f(\alpha) + f \left(\alpha u_{q_j^{(1)}, n} \right) \right). \end{aligned} \quad (4.6)$$

Положим

$$\begin{aligned} X_j^{(1)} &= \{j, j + 2^{n-1}\}, \quad j = 0, \dots, 2^{n-2} - 1, \\ X_j^{(2)} &= X_j^{(1)} \bigcup X_{j+2^{n-2}}^{(1)} = \{j, j + 2^{n-2}, j + 2^{n-1}, j + 2^{n-2} + 2^{n-1}\}, \\ &\quad j = 0, \dots, 2^{n-3} - 1, \end{aligned}$$

зафиксируем набор $\left(q_1^{(2)}, \dots, q_{2^{n-3}}^{(2)} \right)$ и рассмотрим последовательность $\bar{U}^{(2)} = \left(U_0^{(2)}, U_1^{(2)}, \dots, U_{2^{n-3}}^{(2)} \right)$, где $U_0^{(2)} = U_{2^{n-2}}^{(1)}$ и $U_{2^{n-3}}^{(2)}$ – множество орбит ядра $\text{Ker } \varphi_{n-2}^{(G_n)}$,

$$U_j^{(2)} = \left(U_{j-1}^{(2)} \setminus \left\{ X_j^{(1)}, X_{j+2^{n-2}}^{(1)} \right\} \right) \bigcup X_j^{(2)}, \quad j = 1, \dots, 2^{n-3} - 1.$$

Согласно утверждению 4.1 последовательность $\bar{U}^{(2)}$ является неуплотняемой G_n -последовательностью и

$$U_{2^{n-2}}^{(1)} \prec U_1^{(2)} \prec \dots \prec U_{2^{n-3}-1}^{(2)} \prec W^{(n-2,n)}.$$

Тогда существует такая последовательность подгрупп

$$\overline{H}^{(2)} = \left(\text{Ker } \varphi_{n-1}^{(G_n)}, H_1^{(2)}, \dots, H_{2^{n-3}-1}^{(2)}, \text{Ker } \varphi_{n-2}^{(G_n)} \right),$$

что $U_i^{(2)} = O(H_i^{(2)})$, $i = 1, \dots, 2^{n-3} - 1$. Нетрудно убедиться, что для $c = 1, \dots, 2^{n-3}$ справедливы равенства

$$\begin{aligned} f^{(2)}(\alpha) &= \Delta_{H_c^{(2)}}^+ \left(\dots \Delta_{H_2^{(2)}}^+ \left(\Delta_{H_1^{(2)}}^+ f^{(1)}(\alpha) \right) \right) =_{2^n} \\ &=_{2^n} \begin{cases} 2^{j+c-j} \sum_{\beta \in \alpha^{H_c^{(2)}}} \left(\sum_{\lambda \in \beta^{H_1^{(2)}}} f^{(1)}(\lambda) \right), \exists j \in \{0, \dots, c-1\} : |\alpha^{H_j^{(2)}}| = 2, \\ |\alpha^{H_{j+1}^{(2)}}| = 4, \\ 2 \left(\sum_{\beta \in \alpha^{H^{(2)}}} f^{(1)}(\beta) \right), |\alpha^{H_1^{(2)}}| = |\alpha^{H_2^{(2)}}| = \dots = |\alpha^{H^{(2)}}| = 2. \end{cases} \end{aligned} \quad (4.7)$$

Из (4.6) следует, что для любого $\alpha \in \mathbb{Z}_{2^n}$ справедливо равенство

$$f^{(1)}(\alpha) =_2 \begin{cases} f(\alpha) + f\left(\alpha u_{q_{2^{n-2}}, n}^{(1)}\right), & \text{если } \left| \alpha \left\langle u_{q_{2^{n-2}}, n}^{(1)} \right\rangle \right| = 2, \\ 0, & \text{если } \left| \alpha \left\langle u_{q_{2^{n-2}}, n}^{(1)} \right\rangle \right| = 1. \end{cases} \quad (4.8)$$

Таким образом, при $c = n$ из равенств (4.7) и (4.8) имеем

$$\Delta_{H_c^{(2)}}^+ \left(\dots \Delta_{H_2^{(2)}}^+ \left(\Delta_{H_1^{(2)}}^+ f^{(1)}(\alpha) \right) \right) =_{2^n} 0.$$

Значит, $d_{G_n}^{+(1)}(f, \overline{U}) \leq 2^{n-2} + n$.

Так как для любого $\alpha \in V_n$ справедливо равенство

$$\begin{aligned} f'^{(1)}(\alpha) &= \Delta_{\text{Ker } \varphi_{n-1}^{(G_n)}}^\oplus \left(\Delta_{H_{2^{n-2}-1}^{(1)}}^\oplus \left(\dots \Delta_{H_2^{(1)}}^\oplus \left(\Delta_{H_1^{(1)}}^\oplus f(\alpha) \right) \right) \right) = \\ &= \begin{cases} f(\alpha) \oplus f\left(\alpha b_{q_{2^{n-2}}}^{(1)}\right), & \text{если } \left| \alpha \left\langle u_{q_{2^{n-2}}, n}^{(1)} \right\rangle \right| = 2, \\ 0, & \text{если } \left| \alpha \left\langle u_{q_{2^{n-2}}, n}^{(1)} \right\rangle \right| = 1, \end{cases} \end{aligned}$$

то

$$f'^{(1)}(\alpha) = \Delta_{H_1^{(2)}}^\oplus f'^{(1)}(\alpha) = \bigoplus_{\beta \in \alpha^{H_1^{(2)}}} f'^{(1)}(\beta) = 0.$$

Отметим, что для группы P_n значение $d_{P_n}^{*(1)}(f, \bar{U})$ находится аналогичным образом. При этом число 2^{n-2} заменяется числом 2^{n-1} , что следует из утверждения 4.1. Таким образом, $d_{P_n}^{+(1)}(f, \bar{U}) \leq 2^{n-1} + n$, $d_{P_n}^{\oplus(1)}(f, \bar{U}) \leq 2^{n-1} + 1$.

Утверждение доказано.

Пусть $*$ $\in \{+, \oplus\}$. Из утверждения 4.2 следует, что для $f \in (F^\times)_{n,m}^*$ справедливо неравенство

$$1 \leq d_{B,\min}^{*(1)}(f) \leq d_{B,\max}^{*(1)}(f) \leq l_B^*.$$

В случае $\sum_{\beta \in \alpha^{\text{Ker } \varphi_{n-1}^{(G_n)}}} f(\beta) \equiv 1 \pmod{2}$ из доказательства утверждения 4.2 следует, что $d_{B,\max}^{*(1)}(f) = l_B^*$.

Пусть $B \in \{G_n, P_n\}$. Для бинарной операции $*$ $\in \{+, \oplus\}$ найдём величины $d_{B,\min}^{*(1)}(f)$, $d_{B,\max}^{*(1)}(f)$ для двух классов функций $f \in F_{n,m}^*$. К первому классу относятся функции, сумма значений которых на каждой орбите группы $R \in \{\text{Ker } \varphi_{n-1}^{(G_n)}, \text{Ker } \varphi_{n-1}^{(P_n)}\}$ относительно операции $*$ равна нулю. Второй класс состоит из константных отображений.

Пример 4.1. 1. Пусть $A \subseteq \{0, \dots, 2^{n-2} - 1\}$, $F_{n,m}^{*(A,G_n)}$ – такое множество функций, что выполняются условия:

- а) $f(\alpha) \neq 0$ и $f(\alpha) * f(\alpha + 2^{n-1}) = 0$ для каждого $\alpha \in A$;
- б) $f(\beta) = 0$ для каждого $\beta \in \{0, \dots, 2^n - 1\} \setminus (A \cup \{A + 2^{n-2}\})$;
- в) $f(\alpha) * f(\alpha + 2^{n-1}) = 0$ для каждого $\alpha \in \{\beta + 2^{n-2} | \beta \in A\}$.

Тогда $d_{G_n,\min}^{*(1)}(f) = |A|$, $d_{G_n,\max}^{*(1)}(f) = 2^{n-2}$ для произвольной функции $f \in F_{n,m}^{*(A,G_n)}$.

2. Пусть $A' \in \{0, \dots, 2^{n-1} - 1\}$, $F_{n,m}^{*(A',P_n)}$ – такое множество функций, что выполняются условия:

- а) $f(\alpha) \neq 0$ и $f(\alpha) * f(\alpha + 2^{n-1}) = 0$ для каждого $\alpha \in A'$;
- б) $f(\beta) = 0$ для каждого $\beta \in \{0, \dots, 2^n - 1\} \setminus A'$.

Тогда $d_{P_n,\min}^{*(1)}(f) = |A'|$, $d_{P_n,\max}^{*(1)}(f) = 2^{n-1}$ для произвольной функции $f \in F_{n,m}^{*(A',P_n)}$.

Заметим, что Δ^* -степень функции $f \in F_{n,m}^{*(A,G_n)} \cup F_{n,m}^{*(A',P_n)}$ равна 1, т.е. $d^+(f) = d^\oplus(f) = 1$.

3. Пусть $f(x) = b$, $b \neq 0$. Тогда $d^\oplus(f) = d^+(f) = 0$. Из равенств (4.5) и (4.7) следует, что

$$d_{B,\min}^{\oplus(1)}(f) = d_{B,\max}^{\oplus(1)}(f) = \begin{cases} 2^{n-2}, & \text{если } B = G_n, \\ 2^{n-1}, & \text{если } B = P_n, \end{cases}$$

$$d_{B,\min}^{+(1)}(f) = d_{B,\min}^{\oplus(1)}(f) + n - \|b\| - 1,$$

$$d_{B,\max}^{+(1)}(f) = d_{B,\max}^{\oplus(1)}(f) + n - \|b\|.$$

Заметим, что из пп.1–3 примера 4.1 следует, что $d^+(f) \leq d_{G_n, \min}^{*(1)}(f)$.

Приводимое далее утверждение 4.3 позволяет для группы $B \in \{G_n, P_n\}$ и функции $f \in F_{n,1}^\oplus$ находить точное значение величины $d_{B, \min}^{\oplus(1)}(f)$. Кроме того, величина $d_{B, \max}^{\oplus(1)}(f)$ может принимать только два значения.

Для функции $f \in F_{n,1}^\oplus$ и вектора $(\delta_1, \delta_0, \delta'_1, \delta'_0) \in V_4$ положим

$$R_f^\oplus(\delta_1, \delta_0, \delta'_1, \delta'_0) = \left\{ \alpha \in \langle \varepsilon_{n-3,n}, \dots, \varepsilon_{0,n} \rangle \left| \begin{array}{l} f(\alpha), f(\alpha \oplus \varepsilon_{n-1,n}), f(\alpha \oplus \varepsilon_{n-2,n}), \\ f(\alpha \oplus \varepsilon_{n-2,n} \oplus \varepsilon_{n-1,n}) = (\delta_1, \delta_0, \delta'_1, \delta'_0) \end{array} \right. \right\},$$

$$r_{1,f}^{(G_n)} = \sum_{(\delta_1, \delta_0, \delta'_1, \delta'_0) \in V_4: \{0,1\} = \{\delta_1, \delta_0\} \vee \{0,1\} = \{\delta'_1, \delta'_0\}} \left| R_f^\oplus(\delta_1, \delta_0, \delta'_1, \delta'_0) \right|,$$

$$r_{2,f}^{(G_n)} = \left| R_f^\oplus(0, 0, 1, 1) \right| + \left| R_f^\oplus(1, 1, 0, 0) \right| + \left| R_f^\oplus(1, 1, 1, 1) \right|,$$

$$r_{2,f}^{(P_n)} = |\{ \alpha \in \langle \varepsilon_{n-2,n}, \varepsilon_{n-3,n}, \dots, \varepsilon_{0,n} \rangle \mid (f(\alpha), f(\alpha \oplus \varepsilon_{n-1,n})) = (1, 1) \}|.$$

Утверждение 4.3. Пусть $n \geq 2$, $*$ $\in \{+, \oplus\}$, $B \in \{G_n, P_n\}$, $f \in (F^\times)_{n,1}^\oplus$. Тогда

$$d_{B, \min}^{\oplus(1)}(f) = \begin{cases} r_{1,f}^{(B)} + r_{2,f}^{(B)}, & \text{если } r_{2,f}^{(B)} > 0, \\ r_{1,f}^{(B)} + 1, & \text{если } r_{2,f}^{(B)} = 0, \end{cases}$$

$$d_{G_n, \max}^{\oplus(1)}(f) \in \{2^{n-2}, 2^{n-2} + 1\}, \quad d_{P_n, \max}^{\oplus(1)}(f) \in \{2^{n-1}, 2^{n-1} + 1\}.$$

Доказательство. Доказательство следует из того, что если $R \in \{ \text{Кер } \varphi_{n-1}^{(G_n)}, \text{Кер } \varphi_{n-1}^{(P_n)} \}$, то для произвольной неуплотняемой R -последовательности $\bar{H} = (\langle e \rangle, H_1, \dots, H_{l_R-1}, \text{Кер } \varphi_{n-1}^{(R)})$ справедливо равенство

$$\begin{aligned} \Delta_{\text{Кер } \varphi_{n-1}^{(R)}}^\oplus \left(\Delta_{H_{l_R-1}}^\oplus \left(\dots \Delta_{H_2}^\oplus \left(\Delta_{H_1}^\oplus f(x) \right) \right) \right) &= \\ = \begin{cases} f(x) \oplus f(x \oplus \varepsilon_{n-1,n}), & \text{если } x^{H_{l_R-1}} = \{x\}, \\ 0, & \text{если } x^{H_{l_R-1}} \neq \{x\}. \end{cases} \end{aligned} \quad (4.9)$$

С помощью утверждения 4.3 далее получены оценки величин $d_{B, \min}^{\oplus(1)}(f)$, $d_{B, \max}^{\oplus(1)}(f)$ для произвольной функции $f \in F_{n,m}^\oplus$ через её координатные функции. Также оно позволяет описать функции $f \in F_{n,m}^\oplus$, у которых $d_{B, \min}^{\oplus(1)}(f) = d_{B, \max}^{\oplus(1)}(f)$.

Пусть $f_i : V_n \rightarrow \{0, 1\}$ – i -я координатная функция функции $f \in (F^\times)_{n,1}^*$, $i = 0, \dots, n-1$.

Следствие 4.2. Пусть $n \geq 2$, $*$ $\in \{+, \oplus\}$, $B \in \{G_n, P_n\}$, $f \in (F^\times)_{n,1}^*$. Тогда:

- 1) если функция f такова, что $f(\alpha) \oplus f(\alpha \oplus \varepsilon_{n-1,n}) \neq \vec{0}_m$ для каждого $\alpha \in V_n$, то $d_{B, \min}^{\oplus(1)}(f) = d_{B, \max}^{\oplus(1)}(f)$;

2) справедливы соотношения

$$\max \left\{ d_{B,\min}^{\oplus(1)}(f_i) \mid i = 0, \dots, m-1 \right\} \leq d_{B,\min}^{\oplus(1)}(f) \leq l_B^{\oplus},$$

$$d_{B,\max}^{\oplus(1)}(f) \in \{l_B^{\oplus} - 1, l_B^{\oplus}\};$$

3) для каждого числа $j \in \{1, \dots, l_B^{\oplus}\}$ существует такая функция $g \in F_{n,m}^{\oplus}$, что $d_{B,\min}^{\oplus(1)}(g) = j$.

Доказательство следует из равенства (4.9), утверждения 4.3 и пп. 1, 2 примера 4.1.

Для группы $B \in \{G_n, P_n\}$ и функции $f \in F_{n,m}^+$ приведем оценки величин $d_{B,\min}^{+(1)}$, $d_{B,\max}^{+(1)}$.

Утверждение 4.4. Пусть $n \geq 2$, $*$ $\in \{+, \oplus\}$, $B \in \{G_n, P_n\}$, $f \in (F^\times)_{n,m}^*$. Тогда:

- 1) если функция f такова, что $f(\alpha) + f(\alpha + 2^{n-1}) \neq_{2^{m-1}} 0$ для каждого $\alpha \in \{0, \dots, 2^{n-1} - 1\}$, то $d_{B,\min}^{+(1)}(f) \in \{l_B^+ - 1, \dots, d_{B,\max}^{+(1)}(f)\}$;
- 2) справедливо включение $d_{B,\max}^{+(1)}(f) \in \{l_B^+ - n, \dots, l_B^+\}$;
- 3) для каждого числа $j \in \{1, \dots, l_B^+\}$ и $j' \in \{l_B^+ - n, \dots, l_B^+\}$ существуют такие функции $g, g' \in F_{n,m}^+$, что $d_{B,\min}^{+(1)}(g) = j$, $d_{B,\max}^{+(1)}(g') = j'$.

Доказательство. Доказательство следует из равенств (4.5) и (4.7).

Таким образом, величины $d_{B,\min}^{*(1)}(f)$, $d_{B,\max}^{*(1)}(f)$ несложно найти, используя равенства (4.5), (4.7) или (4.9). При этом числа различных значений, принимаемых $d_{B,\min}^{*(1)}(f)$, $d_{B,\max}^{*(1)}(f)$, различны. Так, из следствия 4.2 вытекает, что величина $d_{B,\min}^{\oplus(1)}$ может принимать $l_B^{\oplus}$ разных значений, а $d_{B,\max}^{\oplus(1)}$ — только два. Кроме того, из утверждения 4.4 следует, что $d_{B,\min}^{+(1)}$ принимает l_B^+ различных значений, а $d_{B,\max}^{+(1)}$ принимает $n+1$ значений. Большее число значений, принимаемых $d_{B,\min}^{+(1)}$, $d_{B,\max}^{+(1)}$, связано с тем, что порядки элементов в аддитивной группе $\mathbb{Z}_{2^n}^+$ больше, чем в V_n^+ .

Нетрудно убедиться, что для произвольных $a \in \mathbb{Z}_{2^n}^\times$, $*$ $\in \{+, \oplus\}$, $f, f' \in (F^\times)_{n,m}^*$ справедливы неравенства

$$d_{B,\min}^{+(1)}(af) \leq d_{B,\min}^{+(1)}(f), \quad d_{B,\max}^{+(1)}(af) \leq d_{B,\max}^{+(1)}(f),$$

$$d_{B,\min}^{*(1)}(f * f') \leq d_{B,\min}^{*(1)}(f) + d_{B,\min}^{*(1)}(f'),$$

$$d_{B,\max}^{*(1)}(f * f') \leq d_{B,\max}^{*(1)}(f) + d_{B,\max}^{*(1)}(f').$$

Отметим, что могут выполняться оба неравенства

$$d_{B,\min}^{*(1)}(f * f') \leq \max \left\{ d_{B,\min}^{*(1)}(f), d_{B,\min}^{*(1)}(f') \right\}, \quad (4.10)$$

$$\max \left\{ d_{B,\min}^{*(1)}(f), d_{B,\min}^{*(1)}(f') \right\} \leq d_{B,\min}^{*(1)}(f * f'). \quad (4.11)$$

Неравенства, аналогичные неравенствам (4.10), (4.11), справедливы для величины $d_{B,\max}^{*(1)}(f * f')$.

5. Степень асимметричности 2-го типа и её свойства

Пусть $B \in \{G_n, P_n\}$, $* \in \{+, \oplus\}$. Так как $\Delta_{G_n}^* f(x)$, $\Delta_{P_n}^* f(x)$ – константные отображения, то для каждой функции $f \in F_{n,m}^*$ и неуплотняемой B -последовательности $\bar{U} = (U^{(1)}, \dots, U^{(l_B)})$, где $H_i \leq B$, $U^{(i)} = O(H_i)$, $i = 1, \dots, l_B$, существует такое минимальное число $c \in \{1, \dots, l_B\}$, что $\Delta_{H_j}^* f$ – константное отображение для $j = c, \dots, l_B$. В этом случае положим $d_B^{*(2)}(f, \bar{U}) = c$.

Величину

$$d_B^{*(2)}(f) = \min \left\{ d_B^{*(2)}(f, \bar{U}) \mid \bar{U} \in \Omega(B) \right\}$$

назовём степенью асимметричности 2-го типа.

Заметим, что если $d_B^{*(2)}(f) < l_B - 1$, то $\Delta_{H_j}^* f(x) = 0$ для каждого $j \in \{d_B^{*(2)}(f), \dots, l_B\}$.

Множества $U_0^{(n-1)} = \{\alpha \in \mathbb{Z}_{2^n} \mid \alpha \equiv_2 0\}$, $U_1^{(n-1)} = \{\alpha \in \mathbb{Z}_{2^n} \mid \alpha \equiv_2 1\}$ являются орбитами ядер $\text{Ker } \varphi_1^{(P_n)}$ и $\text{Ker } \varphi_1^{(G_n)}$. Положим $U^{(n-1)} = \{U_0^{(n-1)}, U_1^{(n-1)}\}$, $B \in \{G_n, P_n\}$.

Очевидно, что $(\text{Ker } \varphi_1^{(R)})^*$ -производная отображения $f \in F_{n,m}^*$ удовлетворяет условию

$$\Delta_{\text{Ker } \varphi_1^{(R)}}^* f(0) \neq \Delta_{\text{Ker } \varphi_1^{(R)}}^* f(1), \quad (5.1)$$

если

$$\sum_{\beta \in U_0^{(n-1)}} *f(\beta) \neq \sum_{\beta' \in U_1^{(n-1)}} *f(\beta').$$

Таким образом,

$$d_{P_n}^{*(2)}(f) = 2^n - 1 \quad (d_{G_n}^{*(2)}(f) = 2^{n-1})$$

тогда и только тогда, когда f удовлетворяет соотношению (5.1).

Покажем, что получение верхних и нижних оценок для $d_B^{*(2)}(f)$ сводится к нахождению производных по подгруппам группы B , множества орбит которых есть

$$\Theta^{(i)} = \{r \oplus \langle \varepsilon_{n-i,n}, \dots, \varepsilon_{n-1,n} \rangle \mid r \in \{0, \dots, 2^{n-i-1} - 1\}\}, \quad i = 1, \dots, n-1.$$

Утверждение 5.1. Пусть $n \geq 2$, $B \in \{G_n, P_n\}$, $* \in \{+, \oplus\}$, $f \in F_{n,m}^*$ и $\bar{U} = (U^{(1)}, \dots, U^{(l_B)})$ – произвольная неуплотняемая B -последовательность, $H_i \leq B$, $U^{(i)} = O(H_i)$, $i = 1, \dots, l_B$. Пусть также $\sum_{i=1}^{t-1} 2^{n-i} < d_B^{*(2)}(f) \leq \sum_{i=1}^t 2^{n-i}$ для некоторого $t \in \{1, \dots, n-1\}$. Тогда $\Delta_{H_j}^* f(x) = 0$ для каждого $j \in \left\{ \sum_{i=1}^t 2^{n-i}, \dots, l_B - 1, l_B \right\}$.

Доказательство. Доказательство следует из утверждения 4.1 и того, что если $p = \sum_{i=1}^t 2^{n-i}$ и $\Delta_{H_p}^* f(x) = 0$, то $\Delta_{H_j}^* f(x) = 0$ для каждого $j \in \{p+1, \dots, l_B\}$.

Таким образом, для нахождения оценок величины $d_B^{*(2)}(f)$ и описания свойств орбитальной производной можно рассматривать последовательность $\bar{\Theta} = (\Theta^{(1)}, \dots, \Theta^{(n)})$, где

$$\Theta^{(i)} = \{r \oplus \langle \varepsilon_{n-i,n}, \dots, \varepsilon_{n-1,n} \rangle \mid r \in \{0, \dots, 2^{n-i-1} - 1\}, i = 1, \dots, n-1, \\ \Theta^{(n)} = \{0, \dots, 2^n - 1\},$$

что позволяет непосредственно переносить ряд результатов из [5] на более общий случай.

Пусть $B \in \{G_n, P_n\}$, $*$ $\in \{+, \oplus\}$ и $f \in S(\mathbb{Z}_{2^n})$. Так как $\sum_{\alpha \in \mathbb{Z}_{2^n}} f(\alpha) = 2^n 2^{n-1}$, то

$$l_B - 1 \leq d_B^{+(2)}(f) \leq l_B.$$

Однако $d_B^{\oplus(2)}(f) \leq l_B - 1$.

Очевидно, что для произвольной функции $f \in F_{n,m}^*$

$$d_{B,\min}^{*(1)}(f) \leq d_B^{*(2)}(f).$$

Для отображения $f \in F_{n,m}^*$ и множества $\Lambda = \{\Lambda_1, \dots, \Lambda_c\}$ всех орбит некоторой группы $H \leq P_n$ положим $\Delta_H^* f_\Lambda(\Lambda_j) = \sum_{\alpha \in \Lambda_j} *f(\alpha)$ для $j = 1, \dots, c$. Пусть также

$$u^*(\Lambda; b) = |\{i \in \{1, \dots, |\Lambda|\} \mid \Delta_H^* f_\Lambda(\Lambda_i) = b\}|, \quad * \in \{+, \oplus\}, \quad b \in X_m^*.$$

Пусть $B \in \{G_n, P_n\}$. Очевидно, что для любой функции $f \in F_{n,m}^+$ существует такое число $c \in \{0, \dots, n\}$, что $\Delta_{\text{Ker } \varphi_{n-c}^{(G_n)}}^+ f(x) = a$ для некоторого $a \in \mathbb{Z}_{2^m}^\times$, где $\text{Ker } \varphi_0^{(G_n)} = G_n$. Поэтому величины $d_B^{+(2)}$, $d_B^{+(2)}(f, \bar{U})$ зависят только от порядка элемента a в группе $\mathbb{Z}_{2^m}^+$ для $\bar{U} \in \Omega(B)$ и числа c . Приведём величину $d_B^{+(2)}(f, \bar{U})$ для такой функции f .

Утверждение 5.2. Пусть $n \geq 2$, $m \in \{1, \dots, n\}$ и функция $f \in F_{n,m}^+$ такова, что $\Delta_{\text{Ker } \varphi_{n-c}^{(G_n)}}^+ f(x) = 2^m a$ для некоторых $a \in \mathbb{Z}_{2^m}^\times$, $c \in \{0, \dots, n-1\}$. Тогда справедливы следующие соотношения.

1) Для произвольной неуплотняемой P_n -последовательности

$$\bar{U} = (U_{2^n}^{(0)}, U_1^{(1)}, \dots, U_{2^{n-1}}^{(1)}, \dots, U_1^{(n-2)}, \dots, U_2^{(n-1)}, \{0, \dots, 2^n - 1\})$$

для каждого $b \in {}_{2^m}\mathbb{Z}_{2^m} \setminus \{a, 2a\}$ и $j \in \{1, \dots, 2^{n-c-1}\}$ выполняются равенства

$$u^+(U_j^{(c+1)}; a) = 2^{n-c-1} - j, \quad u^+(U_j^{(c+1)}; 2a) = j, \quad u^+(U_j^{(c+1)}; b) = 0.$$

В частности,

$$d_{P_n}^{+(2)}(f, \bar{U}) = \sum_{j=1}^{c+m-||a||} 2^{n-j}.$$

- 2) Для произвольной неуплотняемой G_n -последовательности $\bar{U}$ справедливо равенство

$$d_{G_n}^{+(2)}(f, \bar{U}) = \sum_{j=1}^{c+m-||a||} 2^{n-j-1}.$$

Доказательство. Доказательство следует из утверждения 4.1 и того, что для каждого $t \in \{0, \dots, n-c\}$ выполняется равенство

$$\Delta_{\text{Ker } \varphi_{n-c-t}^{(P_n)}}^+ f(x) = \Delta_{\text{Ker } \varphi_{n-c-t}^{(G_n)}}^+ f(x) = 2^m a 2^t.$$

Так как $d_B^{*(2)}(f)$ – наименьшее число $d_B^{*(2)}(f, \bar{U})$ среди всех неуплотняемых B -последовательностей $\bar{U} \in \Omega(B)$, то будем сравнивать величины $d_B^{*(2)}(f)$, $d_{B, \min}^{*(1)}(f)$. Найдём $d_B^{*(2)}(f)$ для функций, приведённых в примере 4.1, и сравним с найденной в нём величиной $d_{B, \min}^{*(1)}(f)$.

Пример 5.1. Пусть $*$ $\in \{+, \oplus\}$, $f \in F_{n, m}^*$.

- 1) Для произвольной функции $f \in F_{n, m}^{*(A, B)}$ из пп. 1, 2 примера 4.1 несложно показать, что $d_B^{*(2)}(f) = d_{B, \min}^{*(1)}(f) = |A|$.
- 2) Пусть $f(x) = b$, $b \neq 0$. Тогда

$$d_B^{+(2)}(f) = \begin{cases} \sum_{j=1}^{m-||b||} 2^{n-j-1}, & \text{если } B = G_n, \\ \sum_{j=1}^{m-||b||} 2^{n-j}, & \text{если } B = P_n. \end{cases}$$

Из примеров 4.1, 5.1 видно, что в рассматриваемом случае выполняется неравенство $d_{B, \min}^{+(1)}(f) \leq d_B^{+(2)}(f)$. Заметим, что согласно утверждению 4.1 и следствию 4.2 для $f \in (F^\times)_{n, m}^*$ наибольшее значение $d_{B, \min}^{+(1)}(f)$ равно $l_B^+ \in \{2^{n-2} + n, 2^{n-1} + n\}$, а $d_B^{+(2)}(f) - l_B \in \{2^{n-1} + 1, 2^n\}$. Наименьшее значение у обеих величин $d_{B, \min}^{+(1)}(f)$, $d_B^{+(2)}(f)$ равно 1. Отметим, что $d_{B, \max}^{+(1)}(f) \in \{l_B^+ - n, \dots, l_B^+\}$ принимает $n+1$ различных значений. Таким образом, спектр значений, принимаемых величиной $d_B^{+(2)}(f)$, богаче, чем у величин $d_{B, \min}^{+(1)}(f)$, $d_{B, \max}^{+(1)}(f)$. Однако в отличие от них величину $d_B^{+(2)}(f)$ находить сложнее.

Нетрудно убедиться, что для любых $a \in \mathbb{Z}_{2^n}^\times$ и функций $f, f' \in (F^\times)_{n, m}^*$ справедливы неравенства

$$d_B^{+(2)}(af) \leq d_B^{+(2)}(f), \quad d_B^{*(2)}(f * f') \leq d_B^{*(2)}(f) + d_B^{*(2)}(f').$$

6. Степень асимметричности 3-го типа и её свойства

Приведём еще один аналог понятия «степени нелинейности».

Пусть $B \leq S(V_n)$, $*$ $\in \{+, \oplus\}$, $1 \leq m \leq n$, $f \in F_{n, m}^*$.

Назовём последовательность подгрупп $\bar{H} = H_0 = \langle e_n \rangle, H_1, \dots, H_c$ в группе B , где $(H_i \triangleleft B) H_0 < H_1 < \dots < H_c \leq B$, (нормальной) $B_f^{(c)}$ -последовательностью, если одновременно выполняются условия:

- 1) $\Delta_{H_{i+1}}^* f(x) = \Delta_H^* f(x)$ для каждой подгруппы H , $H_i < H < H_{i+1}$ ($H \triangleleft B$), и каждого $i \in \{0, \dots, c-1\}$;
- 2) $\Delta_{H_i}^* f(x) \neq \Delta_{H_{i+1}}^* f(x)$ для каждого $i \in \{0, \dots, c-1\}$;
- 3) $\Delta_{H_{c-1}}^* f$ не является константным отображением;
- 4) $\Delta_{H_c}^* f$ – константное отображение.

Заметим, что элементы $B_f^{(c)}$ -последовательности $H_1, \dots, H_c$ являются максимальными подгруппами G_n , для которых производная равна $\Delta_{H_{i+1}}^* f(x)$, т.е. $\Delta_{H_{i+1}}^* f(x) = \Delta_H^* f(x)$ для каждой подгруппы H , $H_i < H < H_{i+1}$. Очевидно, что (нормальная) $B_f^{(c)}$ -последовательность существует не для каждого числа $c \in \mathbb{N}$.

Через $d_{B,\min}^{*(3)}(f)$ ($d_{B,\max}^{*(3)}(f)$) обозначим наименьшее (наибольшее) число $c \in \mathbb{N}$, для которого существует $B_f^{(c)}$ -последовательность.

Для константного отображения f положим $d_{B,\min}^{*(3)}(f) = d_{B,\max}^{*(3)}(f) = 0$.

Пусть также $\tilde{d}_{\min}^{*(3)}(f, B)$ ($\tilde{d}_{\max}^{*(3)}(f, B)$) – наименьшее (наибольшее) число $c \in \mathbb{N}$, для которого существует нормальная $B_f^{(c)}$ -последовательность.

Из равенства (4.6) в [5] следует, что в группе G_n для каждой подгруппы H , $\text{Ker } \varphi_{n-i}^{(G_n)} < H < \text{Ker } \varphi_{n-i-1}^{(G_n)}$, $H \triangleleft G_n$, выполняется равенство

$$O(H) = O\left(\text{Ker } \varphi_{n-i-1}^{(G_n)}\right) = W^{(n-i-1, n)}.$$

Пусть $*$ $\in \{\oplus, +\}$. Отметим, что если $\Delta_{\text{Ker } \varphi_{n-t}^{(G_n)}}^* b(x) = \Delta_{\text{Ker } \varphi_{n-t-1}^{(G_n)}}^* b(x)$ для некоторых $t \in \{1, \dots, n-1\}$, $b \in F_{n,m}^*$, то $\Delta_{\text{Ker } \varphi_{n-t-1}^{(G_n)}}^* b(x) = 0$. Это следует из того, что так как

$$\Delta_{\text{Ker } \varphi_{n-t-1}^{(G_n)}}^* b(x) = \Delta_{\text{Ker } \varphi_{n-t}^{(G_n)}}^* b(x) * \Delta_{\text{Ker } \varphi_{n-t}^{(G_n)}}^* b(x \oplus \varepsilon_{n-t-1, n}),$$

то $\Delta_{\text{Ker } \varphi_{n-t}^{(G_n)}}^* b(x) = 0$, а значит, $\Delta_{\text{Ker } \varphi_{n-t-1}^{(G_n)}}^* b(x) = 0$.

Таким образом, нормальной $(G_n)_f^{(c)}$ -последовательностью является единственная последовательность $(\langle e_n \rangle, \text{Ker } \varphi_{n-1}^{(G_n)}, \text{Ker } \varphi_{n-2}^{(G_n)}, \dots, \text{Ker } \varphi_{n-c}^{(G_n)})$,

$$\langle e_n \rangle < \text{Ker } \varphi_{n-1}^{(G_n)} < \dots < \text{Ker } \varphi_{n-c}^{(G_n)} < G_n,$$

и

$$\tilde{d}_{\max}^{*(3)}(f, G_n) = \tilde{d}_{\min}^{*(3)}(f, G_n).$$

В частности,

$$\tilde{d}_{\max}^{+(3)}(f, G_n) = \tilde{d}_{\min}^{+(3)}(f, G_n) = d^+(f).$$

Пусть $B \in \{G_n, P_n\}$. Приведём соотношения между величинами $d_B^{*(2)}(f)$, $d_{B,\min}^{*(3)}(f)$, $d_{B,\max}^{*(3)}(f)$. Нетрудно проверить, что справедливы неравенства

$$1 \leq d_{B,\min}^{*(3)}(f) \leq d_{B,\max}^{*(3)}(f) \leq l_B,$$

$$d_{B,\min}^{\oplus(3)}(f) \leq d_B^{\oplus(2)}(f) \leq d_{B,\max}^{\oplus(3)}(f).$$

Однако, как будет показано в примере 6.1, существуют функции $f \in F_{n,m}^+$, удовлетворяющие обоим неравенствам $d_B^{+(2)}(f) > d_{B,\max}^{+(3)}(f)$, $d_B^{+(2)}(f) \leq d_{B,\max}^{+(3)}(f)$.

Из определений $d_B^{*(2)}(f)$ и $d_{B,\min}^{*(3)}(f)$, $d_{B,\max}^{*(3)}(f)$ следует, что если функции $f \in F_{n,m}^*$ и неуплотняемой B -последовательности $\bar{U} = (U_1, \dots, U_{l_B})$ соответствует такая последовательность подгрупп $\bar{H} = (H_1, \dots, H_{l_B})$, что $U_i = O(H_i)$ для $i = 1, \dots, l_B$ и $\bar{H}^{(c)} = (H_1, \dots, H_c)$ является $B_f^{(c)}$ -последовательностью, причём $H_c = \text{Ker } \varphi_{n-j}^{(G_n)}$ для некоторого $j \in \{1, \dots, n-1\}$, то

- 1) $d_B^{\oplus(2)}(f) \leq c \leq d_{B,\min}^{\oplus(3)}(f)$, $d_B^{\oplus(2)}(f) \leq c \leq d_{B,\max}^{\oplus(3)}(f)$;
- 2) $d_{B,\min}^{+(3)}(f) \leq d_B^{+(2)}(f) \leq c$, $c \leq d_{B,\max}^{+(3)}(f) \leq d_B^{+(2)}(f)$.

Пусть $B \in \{G_n, P_n\}$. Найдём величину $d_{B,\min}^{*(3)}$ для отображений из $F_{n,m}^*$, «близких» к константным. Заметим, что нахождение $d_{B,\max}^{*(3)}$ сложнее, чем $d_{B,\min}^{*(3)}$.

Пусть 0_m – нулевой вектор из $\{0, 1\}^m$.

Утверждение 6.1. Пусть $*$ $\in \{\oplus, +\}$, $f \in F_{n,m}^*$ и существуют такое множество $J_f \subseteq \{0, \dots, 2^{n-1} - 1\}$ и элемент $\delta \in \{0, 1\}^m \setminus \{0_m\}$, что выполняются условия:

- 1) $\sum_{\alpha \in W_j^{(n-1,n)}} *f(\alpha) = \delta$ для каждого $j \in J_f$;
- 2) $f(\beta) = \delta$ для каждого $\beta \notin \bigcup_{i \in J_f} W_i^{(n-1,n)}$.

Тогда $d_{P_n,\min}^{*(3)}(f) = |J_f|$, $d_{P_n,\min}^{\oplus(2)}(f) = |J_f| + 2^{n-1}$.

Доказательство. Пусть $c = |J_f|$, $J_f = \{j_1, j_2, \dots, j_c\}$. Рассмотрим ряд подгрупп $\bar{H} = (H_1^{(1)}, H_2^{(1)}, \dots, H_c^{(1)})$, где

$$H_t^{(1)} = \langle (j_i, 2^{n-1} + j_i) | i \in \{1, \dots, t\} \rangle, \quad t = 1, \dots, c.$$

Ясно, что $\langle e_n \rangle < H_1^{(1)} < H_2^{(1)} < \dots < H_c^{(1)}$ и $\Delta_{H_i^{(1)}}^* f(x) \neq \Delta_{H_{i+1}^{(1)}}^* f(x)$ для $i = 1, \dots, c-1$.

Кроме того, для каждого $i \in \{1, \dots, c-1\}$ не существует такой подгруппы R_i , что $H_i^{(1)} < R_i < H_{i+1}^{(1)}$. Таким образом, из равенства $\Delta_{H_c^{(1)}}^* f(x) = \delta$ следует, что $d_{P_n,\min}^{*(3)}(f) = |J_f|$.

Утверждение доказано.

В частности, для функции f , удовлетворяющей условиям утверждения 6.1, справедливы оценки $d_{*,P_n,\min}^{(3)}(f) \leq 2^{n-1}$. Кроме того, так как

$$\Delta_{\text{Ker } \varphi_{n-1}^{(P_n)}}^{\oplus} f(x) = \Delta_{\text{Ker } \varphi_{n-1}^{(G_n)}}^{\oplus} f(x) = \begin{cases} \delta, & \text{если } x \in \bigcup_{j \in J_f} W_j^{(n-1,n)}, \\ 0, & \text{если } x \notin \bigcup_{j \in J_f} W_j^{(n-1,n)}, \end{cases} \quad (6.1)$$

то

$$d_{G_n,\min}^{*(3)}(f) + 2^{n-1} \leq d_{P_n}^{\oplus(2)}(f) \leq d_{P_n}^{+(2)}(f). \quad (6.2)$$

Приведём аналог утверждения 6.1 для группы G_n .

Утверждение 6.2. Пусть $*$ $\in \{\oplus, +\}$, $f \in F_{n,m}^*$ и существуют такое множество $J_f \subseteq \{0, \dots, 2^{n-2} - 1\}$ и элемент $\delta \in \{0, 1\}^m$, что одновременно выполняются условия:

$$1) \sum_{\alpha \in W_j^{(n-1, n)}} *f(\alpha) = \sum_{\alpha \in W_{j+2^{n-2}}^{(n-1, n)}} *f(\alpha) = \delta \text{ для каждого } j \in J_f;$$

$$2) f(\beta) = \delta \text{ для каждого } \beta \notin \bigcup_{i \in J_f} W_i^{(n-2, n)}.$$

Тогда $d_{G_n, \min}^{*(3)}(f) = |J_f|$.

Доказательство. Доказательство практически аналогично доказательству утверждения 6.1, отличие состоит в том, что элементы последовательности подгрупп $\overline{H} = (H_1^{(1)}, H_2^{(1)}, \dots, H_c^{(1)})$ задаются равенствами

$$H_t^{(1)} = \langle (j_i, 2^{n-1} + j_i)(j_i + 2^{n-2}, 2^{n-1} + 2^{n-2} + j_i) | i \in \{1, \dots, t\} \rangle, t = 1, \dots, c.$$

Заметим, что для функции f , удовлетворяющей условиям утверждения 6.2, справедлива оценка $d_{G_n, \min}^{*(3)}(f) \leq 2^{n-2}$, а из равенства (6.1) следует, что

$$d_{G_n, \min}^{*(3)}(f) + 2^{n-2} \leq d_{G_n}^{\oplus(2)}(f) \leq d_{G_n}^{+(2)}(f). \quad (6.3)$$

Пусть $B \in \{G_n, P_n\}$. Из утверждений 6.1, 6.2 следует, что величина $d_{B, \min}^{*(3)}(f)$ может принимать любое значение из множества $\{0, \dots, l_{\text{Ker } \varphi_{n-1}^{(B)}}\}$.

Неравенства (6.2) и (6.3) дают оценки, связывающие величины $d_{B, \min}^{*(3)}(f)$, $d_B^{\oplus(2)}(f)$ и $d_B^{+(2)}(f)$ для функций, описанных в утверждениях 6.1 и 6.2. Видно, что величина $d_B^{*(2)}(f)$ больше величины $d_{B, \min}^{*(3)}(f)$ на число элементов $l_{\text{Ker } \varphi_{n-1}^{(B)}}$ неуплотняемой $\text{Ker } \varphi_{n-1}^{(B)}$ -последовательности. Это обусловлено тем, что если $d_B^{*(2)}(f) < l_B - 1$, то величина $d_B^{*(2)}(f)$ определяется как наименьшая длина l_H такой неуплотняемой R -последовательности $\overline{H} = (\langle e_n \rangle, H_1, \dots, H_{l_R})$, где $R \leq B$ и $H_{l_R} = R$, что $\Delta_R^* f(x) = 0$. Однако возможна ситуация, когда $\Delta_{H_i}^* f(x) = \Delta_{H_j}^* f(x)$ при $1 \leq i < j < l_R$. При определении $d_{B, \min}^{*(3)}(f)$ рассматривается такая $B_f^{(c)}$ -последовательность $\overline{H}' = (H'_1, \dots, H'_c)$, что $\Delta_{H'_i}^* f(x) \neq \Delta_{H'_j}^* f(x)$ при $1 \leq i < j < c$, и $d_{B, \min}^{*(3)}(f)$ равно наименьшему числу $c \in \{1, \dots, l_B\}$, для которого $\Delta_{H'_c}^* f(x)$ – константное отображение. Такое различие в определениях и приводит к неравенствам (6.2), (6.3).

Заметим также, что утверждения 6.1, 6.2 являются аналогами результатов, приведенных в п.1, 2 примера 4.1 для величины $d_{B, \min}^{*(1)}(f)$ и в п.1 примера 5.1 для величины $d_B^{*(2)}(f)$.

Укажем величины $d_{B, \min}^{*(3)}(f)$, $d_{B, \max}^{*(3)}(f)$ для трех классов функций и сравним их с величинами $d_B^{*(2)}(f)$, $d_{B, \min}^{*(1)}(f)$, $d_{B, \max}^{*(1)}(f)$. К первому классу относятся функции, принимающие значение 0 один раз, а все остальные значения равны 1. Противоположная ситуация во втором классе, ему принадлежат функции, принимающие значение 1 ровно один раз, а все остальные значения равны 0. К третьему классу относятся функции, принимающие значение 1 два раза, а все остальные значения равны 0, причем наборы, на которых функция равна 1, разной чётности.

Пример 6.1. Пусть $n \geq 2$, $*$ $\in \{\oplus, +\}$, $f \in F_{n,m}^*$, $\delta_1, \dots, \delta_n \in \{0, 1\}$, $x = x_0 + 2x_1 + \dots + 2^{n-1}x_{n-1}$, где $x_0, \dots, x_{n-1} \in \{0, 1\}$.

1. Если

$$f(x) = \tilde{f}(x_{n-1}, \dots, x_0) = 1 \oplus \prod_{j=0}^{n-1} (x_j \oplus \delta_j),$$

то $d_{P_n, \min}^{*(3)}(f) = 1$, так как $\Delta_H^* f(x) = 1$ для $H = \langle (\delta, 2^{n-1} + \delta) \rangle$, где $\delta = \delta_0 + 2\delta_1 + \dots + 2^{n-1}\delta_{n-1}$. Заметим, что

$$d_{P_n, \min}^{\oplus(1)}(f) = 2^{n-1}, \quad d_{P_n}^{\oplus(2)}(f) = d_{P_n, \max}^{\oplus(1)}(f) = 2^{n-1} + 1.$$

Для нахождения $d_{G_n, \min}^{*(3)}(f)$ рассмотрим последовательность подгрупп

$$\overline{H} = \left(H_1^{(1)}, \dots, H_{2^{n-2}}^{(1)}, H_1^{(2)}, \dots, H_{2^{n-3}}^{(2)}, \dots, H_1^{(n-2)}, H_2^{(n-2)}, H_1^{(n-1)}, G_n \right),$$

множество орбит элементов которой соответствует произвольной неуплотняемой G_n -последовательности

$$\left(O\left(H_1^{(1)}\right), \dots, O\left(H_{2^{n-2}}^{(1)}\right), O\left(H_1^{(2)}\right), \dots, O\left(H_{2^{n-3}}^{(2)}\right), \dots, \right. \\ \left. \dots, O\left(H_1^{(n-2)}\right), O\left(H_2^{(n-2)}\right), O\left(H_1^{(n-1)}\right), \{0, \dots, 2^n - 1\} \right).$$

Нетрудно убедиться, что $\Delta_H^* f(x) \neq \Delta_{H'}^* f(x)$ для любых различных элементов H, H' последовательности $\overline{H}$. Значит,

$$d_{G_n, \min}^{*(3)}(f) = d_{G_n, \max}^{*(3)}(f) = d_{G_n, \max}^{*(1)}(f) = d_{G_n}^{\oplus(2)}(f) = 2^{n-2} + 1.$$

При этом $d_{P_n, \min}^{\oplus(1)}(f) = 2^{n-2}$.

2. Если $B \in \{G_n, P_n\}$,

$$f(x) = \tilde{f}(x_{n-1}, \dots, x_0) = \prod_{j=0}^{n-1} (x_j \oplus \delta_j),$$

то

$$d_{B, \min}^{+(1)}(f) = d_{B, \min}^{+(3)}(f) = d_{B, \max}^{+(3)}(f) = n, \\ d_{B, \min}^{\oplus(1)}(f) = d_{B, \min}^{\oplus(3)}(f) = d_{B, \max}^{\oplus(3)}(f) = 2.$$

Это следует из того, что $\Delta_{\text{Ker } \varphi_{n-i-1}^{(B)}}^+ f(x) \neq \Delta_{\text{Ker } \varphi_{n-i}^{(B)}}^+ f(x)$, $\Delta_{\text{Ker } \varphi_{n-i}^{(B)}}^* f(x) = 1$ и $\Delta_{H^{(n-i)}}^* f(x) = \Delta_{\text{Ker } \varphi_{n-i}^{(B)}}^* f(x)$ для каждой группы $H^{(n-i)}$, $\text{Ker } \varphi_{n-i}^{(B)} \leq H^{(n-i)} < \text{Ker } \varphi_{n-i-1}^{(B)}$, $i = 0, \dots, n-1$.

Пусть $\alpha = \sum_{j=0}^{n-1} \delta_j 2^j$, $\alpha' = {}_{2^n} \alpha + 2^{n-2}$ и $\alpha \in W_t^{(i,n)}$, $\alpha' \in W_q^{(i,n)}$ для некоторых $t, q \in \{0, \dots, 2^{n-i} - 1\}$.

Так как

$$\begin{aligned}
\Delta_{\text{Ker } \varphi_{n-i}^{(P_n)}}^+ f(x) &= \begin{cases} 2^{i-1}, & \text{если } x \in W_t^{(i,n)}, \\ 0, & \text{если } x \notin W_t^{(i,n)}, \end{cases} \\
\Delta_{\text{Ker } \varphi_{n-i}^{(G_n)}}^+ f(x) &= \begin{cases} 2^{i-1}, & \text{если } x \in W_t^{(i,n)} \cup W_q^{(i,n)}, \\ 0, & \text{если } x \notin W_t^{(i,n)} \cup W_q^{(i,n)}, \end{cases} \\
\Delta_{\text{Ker } \varphi_{n-1}^{(P_n)}}^\oplus f(x) &= \begin{cases} 1, & \text{если } x \in W_t^{(1,n)}, \\ 0, & \text{если } x \notin W_t^{(1,n)}, \end{cases} \\
\Delta_{\text{Ker } \varphi_{n-1}^{(G_n)}}^\oplus f(x) &= \begin{cases} 1, & \text{если } x \in W_t^{(1,n)} \cup W_q^{(1,n)}, \\ 0, & \text{если } x \notin W_t^{(1,n)} \cup W_q^{(1,n)}, \end{cases}
\end{aligned}$$

то

$$\begin{aligned}
d_{P_n}^{\oplus(2)}(f) &= d_{P_n, \max}^{+(1)}(f) = 2^{n-1} + 1, \quad d_{P_n}^{+(2)}(f) = \sum_{j=1}^m 2^{n-j}, \\
d_{G_n}^{\oplus(2)}(f) &= d_{G_n, \max}^{+(1)}(f) = 2^{n-2} + 1, \quad d_{G_n}^{+(2)}(f) = \sum_{j=1}^m 2^{n-j-1}.
\end{aligned}$$

3. Пусть $B \in \{G_n, P_n\}$, $\{\alpha_1, \alpha_2\} \subset \{0, \dots, 2^n - 1\}$, $\alpha_0 \equiv_2 0$, $\alpha_1 \equiv_2 1$,

$$f(\beta) = \begin{cases} 1, & \text{если } \beta \in \{\alpha_0, \alpha_1\}, \\ 0, & \text{если } \beta \in \{0, \dots, 2^n - 1\} \setminus \{\alpha_0, \alpha_1\}. \end{cases}$$

Тогда

$$d_{B, \min}^{*(3)}(f) = d_{B, \max}^{*(3)}(f) = n - 1.$$

Это следует из того, что $\Delta_{\text{Ker } \varphi_{n-i-1}^{(B)}}^* f(x) \neq \Delta_{\text{Ker } \varphi_{n-i}^{(B)}}^* f(x)$, $\Delta_{\text{Ker } \varphi_1^{(B)}}^* f(x) = 1$ и $\Delta_{H^{(n-i)}}^* f(x) = \Delta_{\text{Ker } \varphi_{n-i}^{(B)}}^* f(x)$ для каждой группы $H^{(n-i)}$, $\text{Ker } \varphi_{n-i}^{(B)} \leq H^{(n-i)} < \text{Ker } \varphi_{n-i-1}^{(B)}$, $i = 0, \dots, n - 2$.

Пусть $B \in \{G_n, P_n\}$. В примере 6.1 приведены случаи, при которых равны некоторые из величин $d_{B, \min}^{*(1)}(f)$, $d_{B, \max}^{*(1)}(f)$, $d_B^{*(2)}(f)$, $d_{G_n, \min}^{*(3)}(f)$, $d_{G_n, \max}^{*(3)}(f)$.

Из п.1 примера 6.1 следует существование функций $f \in F_{n, m}^\oplus$, для которых

$$d_{G_n, \min}^{*(3)}(f) = d_{G_n, \max}^{*(3)}(f) = d_{G_n, \max}^{*(1)}(f) = d_{G_n}^{\oplus(2)}(f),$$

а из п.2 – существование функций $f \in F_{n, m}^*$, для которых

$$\begin{aligned}
d_{B, \min}^{*(1)}(f) &= d_{B, \min}^{*(3)}(f) = d_{B, \max}^{*(3)}(f), \\
d_B^{\oplus(2)}(f) &= d_{B, \max}^{+(1)}(f).
\end{aligned}$$

Видно, что наибольшее значение принимает величина $d_B^{+(2)}(f)$. При этом в приведенных примерах $d_{B, \max}^{*(3)}(f) \leq d_{B, \max}^{*(1)}(f)$.

Таким образом, рассмотрение всех трёх степеней асимметричности позволяет более тонко различать свойства функций относительно групп G_n , P_n .

Список литературы

1. *Дискретная математика. Энциклопедия*, М.: Научное издательство «Большая Российская энциклопедия», 2004.
2. Cusick T. W., Stănică P., *Cryptographic Boolean Functions and Applications*, Elsevier, 2009, 232 pp.
3. Погорелов Б. А., Пудовкина М. А., “Орбитальные производные над кольцом вычетов. Часть I. Общие свойства”, *Математические вопросы криптографии*, **5**:4 (2014), 99–127.
4. Погорелов Б. А., Пудовкина М. А., “Орбитальные производные над кольцом вычетов. Часть II. Вероятностно-комбинаторные свойства”, *Математические вопросы криптографии*, **6**:1 (2015), 117–133.
5. Погорелов Б. А., Пудовкина М. А., “Орбитальные производные и надгруппы регулярных аддитивных групп”, *Математические вопросы криптографии*, 2015 (в печати).
6. Сачков В. Н., *Введение в комбинаторные методы дискретной математики*, М.: МЦНМО, 2004.
7. Черемушкин А. В., “Аддитивный подход к определению степени нелинейности дискретной функции”, *Прикладная дискретная математика*, 2010, № 2, 22–33.
8. Черемушкин А. В., “Аддитивный подход к определению степени нелинейности дискретной функции на циклической группе примарного порядка”, *Прикладная дискретная математика*, 2013, № 2, 26–38.
9. Черемушкин А. В., “Вычисление степени нелинейности функции на циклической группе примарного порядка”, *Прикладная дискретная математика*, 2014, № 2, 37–47.

Статья поступила 26.12.2014.