УДК 512.54

НЕКОТОРЫЕ ХАРАКТЕРИСТИКИ "НЕЛИНЕЙНОСТИ" ГРУППОВЫХ ОТОБРАЖЕНИЙ *

О.А. ЛОГАЧЕВ, А.А. САЛЬНИКОВ, В.В. ЯЩЕНКО

Введены новые параметры, характеризующие "отклонение" отображений конечных абелевых групп от гомоморфизмов. Эти параметры обобщают известные в теории булевых отображений понятия индекса линейности и максимального элемента таблицы разностей, которые используются в криптографических приложениях. Получены неравенства, связывающие введенные параметры.

1 Определения и обозначения

Всюду ниже будем использовать аддитивную запись для групповых операций, не оговаривая о какой конкретно группе идет речь, кроме тех случаев, где такая вольность в обозначениях может вызвать неоднозначное толкование. Пусть G и H — конечные абелевы группы. Основными объектами, рассматриваемыми в настоящей работе, будут отображения группы G в группу H. Множество всех таких отображений будем обозначать через $H^G = \{\varphi : G \to H\}$. Множество H^G является конечной абелевой группой с операцией поточечного сложения отображений. Иногда отображения $\varphi : G \to H$ удобно представлять в виде векторов с координатами из группы H, которые занумерованы элементами группы G (такое представление отображений будем называть табличным).

В группе отображений H^G выделим подгруппу гомоморфизмов из G в H, обозначенную через $\mathrm{Hom}(G, H)$ (см. [2]). Основная цель настоящей работы состоит в изучении расположения (например, далеко — близко) отображений $\varphi : G \to H$ по отношению к $\mathrm{Hom}(G, H)$. Для придания точного смысла этим утверждениям мы вводим некоторые характеристики отображений, но сначала на H^G вводим подходящие эквивалентности. Через $\mathrm{Aut}(G)$ будем обозначать группу автоморфизмов группы G. На множестве отображений H^G определим отношение эквивалентности.

*Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проекты 99-01-00929 и 99-01-00941).

ОПРЕДЕЛЕНИЕ 1. Отображения φ и ψ из H^G назовем *α-эквивалентными*, если имеются такие автоморфизмы $\omega_1 \in \mathrm{Aut}(G)$, $\omega_2 \in \mathrm{Aut}(H)$ и такие элементы $g \in G$, $h \in H$, что

$$\omega_2\big(\varphi(x)\big) + h = \psi\big(\omega_1(x) + g\big)$$

для любого $x \in G$.

Легко проверить, что так введенное отношение является отношением эквивалентности. В случае отображений пространств над конечным полем α-эквивалентность совпадает с аффинной эквивалентностью (два отображения векторных пространств называются *аффинно эквивалентными*, если одно может быть получено из другого с помощью невырожденной аффинной замены переменных и композиции с невырожденным аффинным отображением). Естественно считать, что α-эквивалентные отображения одинаково расположены относительно $\mathrm{Hom}(G, H)$. Классы α-эквивалентных отображений будем называть *α-классами*. Характеристики отображений, которые постоянны на каждом α-классе (т. е. равны для α-эквивалентных отображений) будем называть *α-инвариантами*. α-инварианты представляют большой интерес для приложений. Примеры α-инвариантов будут приведены ниже.

Любое отображение $\varphi \in H^G$ обычным образом определяет ядерное разбиение группы G на непересекающиеся прообразы $\varphi^{-1}(h)$ элементов h из H, которые называются *блоками ядерного разбиения*. Набор мощностей блоков $\{\, |\varphi^{-1}(h)| \mid h \in H \,\}$ будем называть *весом* отображения φ, а числа $|\varphi^{-1}(h)|$ — элементами веса. Очевидно, что мультимножество элементов веса отображения $\varphi \in H^G$ является α-инвариантом. Поскольку $G = \bigcup\limits_{h \in H} \varphi^{-1}(h)$, то $\sum\limits_{h \in H} \big|\varphi^{-1}(h)\big| = |G|$. Сюръективные отображения, у которых все элементы веса равны, называются *уравновешенными*.

Следующим естественным обобщением α-эквивалентности при изучении свойств и характеристик групповых отображений является рассмотрение произвольных сюръективных гомоморфизмов из групп G и H в некоторые группы G' и H' соответственно и выделение таких свойств, которые сохраняются при гомоморфизмах. При этом воспользуемся стандартным языком теории категорий (см. [2]).

ОПРЕДЕЛЕНИЕ 2. Отображение $\psi : G' \to H'$ *биморфно* отображению $\varphi : G \to H$, если существуют такие сюръективные гомоморфизмы $\omega_1 \in \mathrm{Hom}(G, G')$, $\omega_2 \in \mathrm{Hom}(H, H')$ и константы ${g_0}' \in G'$ и ${h_0}' \in H'$, что диаграмма

$$\begin{array}{ccc} G & \xrightarrow{\ \varphi\ } & H \\ {\scriptstyle \omega_1,\, {g_0}'}\big\downarrow & & \big\downarrow{\scriptstyle \omega_2,\, {h_0}'} \\ G' & \xrightarrow[\ \psi\ ]{} & H' \end{array}$$

коммутативна, т. е.

$$\omega_2\big(\varphi(x)\big) + {h_0}' = \psi\big(\omega_1(x) + {g_0}'\big) \ . \qquad (1)$$

Естественно считать, что если отображение $\psi : G' \to H'$ биморфно отображению $\varphi : G \to H$, то отображения φ и ψ одинаково расположены

относительно $\mathrm{Hom}(G,H)$ и $\mathrm{Hom}(G',H')$ соответственно. Свойства отображений, которые сохраняются при биморфизмах, будем называть *категориальными*. Именно категориальные свойства связаны с расположением отображений относительно $\mathrm{Hom}(G,H)$.

Простейшие примеры категориальных свойств приведены в следующем легко доказываемом утверждении.

ТЕОРЕМА 1. *Категориальными являются следующие свойства отображений* :

1. $\varphi(x) = \mathrm{const}$, *при любом* $x \in G$,
2. $\varphi \in \mathrm{Hom}(G,H)$,
3. *уравновешенность*.

Другие примеры категориальных свойств будут приведены ниже. Отметим, что для булевых отображений категориальными свойствами являются, в частности, свойства, сводимые к свойствам координатных функций (подробнее о таких свойствах см. [6]). Сводимость свойства P булевого отображения означает следующее: булево отображение обладает свойством P тогда и только тогда, когда свойством P обладает любая ненулевая линейная комбинация координатных функций. Известно, что свойства булевых отображений, перечисленные в теореме 1, являются сводимыми.

2 Производные отображений

ОПРЕДЕЛЕНИЕ 3. *Производной* отображения $\varphi \in H^G$ по направлению $a \in G$ называется отображение

$$\frac{d\,\varphi}{d\,a}(x) = \varphi(x+a) - \varphi(x) \ , \tag{2}$$

справедливое при любом $x \in G$.

При этом производная по нулевому направлению является отображением, тождественно равным нулю. В случае, когда группа H совпадает с мультипликативной группой комплексных корней из единицы порядка q, где q — экспонента группы G (т. е. максимальный порядок элементов из G), аппарат производных был развит в работах [4, 3]. Многие из обнаруженных свойств производных достаточно легко переносятся на случай произвольной группы H.

Пусть отображение $\psi : G' \to H'$ биморфно отображению $\varphi : G \to H$, причем биморфизм реализуется с помощью пары гомоморфизмов (ω_1, ω_2) и пары констант $\left({g_0}', {h_0}'\right)$, см. (1). Несложно проверить, что в этом случае при любом направлении $c \in G$ справедливо следующее равенство производных

$$\omega_2\left(\frac{d\varphi}{dc}(x)\right) = \frac{d\psi}{d\omega_1(c)}\left(\omega_1(x) + {g_0}'\right) \ .$$

Другими словами, в этом случае производная отображения ψ по направлению $\omega_1(c) \in G'$ биморфна производной отображения φ по направлению

$c \in G$. Отсюда следует, что если свойства отображений вводятся с помощью категориальных свойств производных, то они оказываются категориальными.

Понятие производной позволяет индуктивным образом ввести вложенную систему подгрупп в группе всех отображений H^G (см. [4]) или, другими словами, расслоить группу H^G. Первым шагом в такой конструкции является отображение тождественно равное нулю на G: положим $RM_{-1}(G,H) = \{\, \varphi \in H^G \mid \varphi(x) = 0 \,\text{при любом}\, x \in G \,\}$. Далее семейства отображений определяются с помощью индуктивного шага:

$$RM_{j+1}(G,H) = \left\{ \varphi \in H^G \mid \frac{d\,\varphi}{d\,c} \in RM_j(G,H), \text{ при любом } c \in G \right\}, \qquad j = -1, 0, 1, 2, \ldots$$

Когда ясно, об отображениях каких групп идет речь, вместо $RM_j(G,H)$ будем писать RM_j. Из теоремы 1, индуктивного процесса построения RM_j и сделанного выше замечания о категориальных свойствах производных следует, что свойство отображений "лежать в множестве RM_j" является категориальным при любом j. Нетрудно понять, что

- для каждого $j = 0, 1, 2, \ldots$ семейство отображений RM_j является подгруппой группы H^G,
- для каждого $j = 0, 1, 2, \ldots$ справедливо вложение $RM_j \subseteq RM_{j+1}$.

Легко проверить, что RM_0 суть константы, а RM_1 суть гомоморфизмы и их сдвиги:

$$RM_1 = \{\, \varphi \in H^G \mid \varphi(x) = \omega(x) + h_0, \text{ для любых } x \in G, \text{ где } \omega \in \mathrm{Hom}(G,H), h_0 \in H \,\} \quad . \qquad (3)$$

В случае, когда G и H являются векторными пространствами над одним и тем же полем, семейство отображений RM_1 является семейством аффинных отображений.

Существуют группы G и H такие, что не всякое отображение из H^G лежит в некотором семействе RM_j (примеры см. в работе [4]). Если же для отображения $\varphi \in H^G$ существует номер j такой, что $\varphi \in RM_j$, то всякое отображение, α-эквивалентное отображению φ, лежит в том же семействе RM_j. В этом случае положим по определению:

$$\deg(\varphi) = \min \{\, j \mid \varphi \in RM_j \,\} \quad .$$

Очевидно, что $\deg(\varphi)$ является α-инвариантом и определенным образом характеризует отклонение отображения φ от RM_1. Отметим, что определение $\deg(\varphi)$ эквивалентно следующему включению:

$$\varphi \in RM_{\deg(\varphi)} \backslash RM_{\deg(\varphi)-1} \quad .$$

Если $\varphi \notin RM_j$ для любого j, то для удобства можно положить $\deg(\varphi) = \infty$. Конечность величины $\deg(\varphi)$ является категориальным свойством. В случае булевых функций (т. е. когда G является векторным пространством над полем из двух элементов, группа $H = \{0,1\}$ является аддитивной

группой того же поля) параметр $\deg(\varphi)$ конечен для всех φ и совпадает со степенью нелинейности. В этом случае введенные семейства отображений RM_j, представленные как множества векторов, являются кодами Рида-Маллера. Различные обобщения кодов Рида-Маллера (групповые коды Рида-Маллера [1]; коды типа Рида-Маллера на конечной абелевой группе [4]) вкладываются в приведенную конструкцию. В случае, когда H и G являются векторными пространствами над одним и тем же полем, параметр $\deg(\varphi)$ не превосходит максимальной степени нелинейности многочленов, реализующих координатные функции отображения φ.

В ряде случаев при изучении отображения $\varphi \in H^G$ оказываются полезными следующие подмножества группы G:

$$L_\varphi^j = \left\{ a \in G \mid \frac{d\,\varphi}{d\,a} \in RM_j \right\}, \quad j = 0, 1, 2, \ldots$$

Из легко проверяемого равенства

$$\frac{d\,\varphi}{d\,(a+b)}(x) = \frac{d\,\varphi}{d\,a}(x) + \frac{d\,\varphi}{d\,b}(x+a)$$

следует, что все подмножества L_φ^j являются подгруппами группы G. В случае булевых функций множества L_φ^j называются пространствами j-нелинейности (см. работу [5]). Для булевых отображений (т. е. отображений линейных пространств над полем из двух элементов) элементы пространства L_φ^0 в криптографической литературе называются линейными трансляторами (см. [10]). Следуя традиции, и в общем случае элементы группы L_φ^0 будем называть *гомоморфными трансляторами*. Из введенных определений следует, что

$$L_\varphi^j = G \Longleftrightarrow \varphi \in RM_{j+1} \ .$$

Очевидно, что при каждом $j = 0, 1, 2, \ldots$ мощность группы L_φ^j является α-инвариантом.

Веса всех производных отображения $\varphi \in H^G$ по ненулевым направлениям можно расположить в виде таблицы R^φ из $|G|-1$ строк и $|H|$ столбцов, в которой строка с номером $x \in G\backslash\{0\}$ состоит из элементов веса отображения $\frac{d\,\varphi}{d\,x}$, т. е. при каждом $x \in G\backslash\{0\}$ и $y \in H$

$$R_{x,y}^\varphi = \left| \left(\frac{d\,\varphi}{d\,x} \right)^{-1} (y) \right| \ .$$

Элементы таблицы R^φ связаны определенными соотношениями. В частности, для любого $x \in G$ справедливо равенство

$$\sum_{y \in H} R_{x,y}^\varphi = |G| \ . \tag{4}$$

В случае, когда отображение φ является составной частью криптографического преобразования, таблица R^φ имеет многочисленные приложения в дифференциальном (разностном) криптоанализе (см. основополагающую работу [9]; дифференциальному криптоанализу постоянно посвящается несколько работ на каждых ежегодных конференциях EUROCRYPT и

CRYPTO). Обычно таблицу R^φ называют таблицей разностей. При оценке эффективности дифференциального метода криптографического анализа используется максимальный элемент таблицы разностей

$$\mu l(\varphi) = \max_{\substack{x \in G \setminus \{0\} \\ y \in H}} R^\varphi_{x,y} \ .$$

Легко проверить, что мультимножество элементов таблицы разностей отображения $\varphi \in H^G$, а значит и ее максимальный элемент $\mu l(\varphi)$, являются α-инвариантами. Величина $\mu l(\varphi)$ определенным образом характеризует отклонение отображения φ от семейства RM_1 (для функций $\psi \in RM_1$ в каждой строке таблицы разностей содержится ровно один ненулевой элемент, равный $|G|$. Поэтому выполнено равенство $\mu l(\psi) = |G|$). Из введенных определений следует, что для некоторого элемента таблицы разностей R^φ равенство $R^\varphi_{a,b} = |G|$ выполнено тогда и только тогда, когда в строке с номером a таблицы R^φ все элементы являются нулевыми кроме $R^\varphi_{a,b}$. Значит, элемент $a \in G$ является гомоморфным транслятором отображения φ. В смысле характеристики μl максимально удаленными от RM_1 и наиболее устойчивыми относительно дифференциального метода криптоанализа являются отображения, минимизирующие величину $\mu l(\varphi)$. Из равенства (4) следует, что для любого отображения $\varphi \in H^G$ выполнено неравенство $\mu l(\varphi) \geqslant |G|/|H|$ (это неравенство нетривиально только в случае $|G| \geqslant |H|$). Если $|H|$ делит $|G|$, то для достижимости указанной оценки необходимо выполнение следующих равенств

$$R^\varphi_{a,b} = \frac{|G|}{|H|}, \text{ при всех } a \in G \setminus \{0\} \text{ и } b \in H \ ,$$

которые означают, что все производные отображения φ по ненулевым направлениям являются уравновешенными отображениями.

В случае, когда φ является булевой функцией, последнее свойство эквивалентно тому, что функция φ является бент-функцией (критерий Ротхауза [11], обзор более поздних исследований по булевым бент-функциям и их обобщениям см. в [3]). Бент-функции на конечной абелевой группе введены в [3], как в свое время и булевы бент-функции, с помощью свойств коэффициентов Фурье, при этом доказанное в [3] обобщение критерия Ротхауза не для всех групп означает " уравновешенность всех производных отображения φ по ненулевым направлениям". Подчеркнем, что свойство отображения φ, выраженное словами в кавычках, является, очевидно, категориальным свойством.

3 Разветвление отображений

Введем новое понятие гомоморфного разветвления отображений. Пусть кроме групп G и H задана еще одна конечная абелева группа K. Пусть также заданы $\rho \in \mathrm{Hom}(G, K)$ и семейство отображений (не обязательно различных) $\{ \alpha_k \in RM_1(G, H) \mid k \in K \}$, заиндексированных элементами группы K. Отображение $\varphi \in H^G$ определим равенством

$$\varphi(x) = \alpha_{\rho(x)}(x) \ . \tag{5}$$

Будем говорить, что φ — *гомоморфное разветвление* с *разветвляющей группой* K и *разветвляющим отображением* ρ. При этом отображение $\alpha_k \in RM_1(G,H)$, $k \in K$ будем называть *разветвляемыми*.

Нетрудно понять, что любое отображение $\varphi \in H^G$ можно представить в виде гомоморфного разветвления. Действительно, достаточно положить $K = G$, $\rho(x) = x$ и $\alpha_k(x) \equiv \varphi(k)$ для всех $x, k \in G$. Очевидно, что при изучении гомоморфных разветвлений в качестве группы K достаточно рассматривать образ группы G при действии отображения ρ: $K = Im_\rho(G)$. Поэтому ниже всюду будем считать, что гомоморфизм ρ сюръективен.

Отметим, что представление отображения в виде гомоморфного разветвления, вообще говоря, не однозначно. Минимальный порядок разветвляющей группы по всем возможным представлениям отображения $\varphi \in H^G$ в виде гомоморфного разветвления назовем *индексом гомоморфности* отображения φ и будем обозначать через $ih(\varphi)$. Легко понять, что индекс гомоморфности отображения является α-инвариантом. Параметр $ih(\varphi)$, как $\deg(\varphi)$ и $\mu l(\varphi)$, определенным образом характеризует отклонение отображения φ от семейства RM_1 (для функций $\psi \in RM_1$, очевидно, выполнено равенство $ih(\varphi) = 1$). В этом смысле максимально удаленными от RM_1 являются отображения, максимизирующие величину $ih(\varphi)$.

Между параметрами $\deg(\varphi)$, $\mu l(\varphi)$ и $ih(\varphi)$ существуют определенные связи. Приведем пример связи между $\deg(\varphi)$ и $ih(\varphi)$ в случае функций на векторных пространствах. Пусть G — векторное пространство размерности s над конечным полем $\mathbb{F}$. Рассмотрим частный случай представления отображения $\varphi : G \to \mathbb{F}$ в виде гомоморфного разветвления, т. е. случай, когда в представлении (5) группа K является векторным пространством над тем же полем $\mathbb{F}$ (такие разветвления называются линейными). В случае, когда $|K| = ih(\varphi)$, размерность пространства K называется *индексом линейности* отображения φ и обозначается через $ill(\varphi)$. Введенные параметры $ill(\varphi)$ и $ih(\varphi)$ связаны равенством $ih(\varphi) = p^{ill(\varphi)}$, где p — характеристика поля $\mathbb{F}$.

Поскольку в этом случае любая функция $\alpha \in RM_1(G,\mathbb{F})$ однозначно представима в виде

$$\alpha(z_1, \ldots, z_s) = a_1 z_1 + \ldots + a_s z_s + b \ ,$$

то нетрудно убедиться в справедливости следующего утверждения.

ЛЕММА 1. *Для отображения $\varphi : G \to \mathbb{F}$ выполнено равенство $ill(\varphi) = t$ тогда и только тогда, когда с помощью некоторой аффинной замены переменных отображение φ может быть представлено в виде*

$$\begin{aligned}\varphi(x_1, \ldots, x_{s-t}, y_1, \ldots, y_t) = \\ = \varphi_1(y_1, \ldots, y_t)\, x_1 + \ldots + \varphi_{s-t}(y_1, \ldots, y_t)\, x_{s-t} + +\psi(y_1, \ldots, y_t) \ .\end{aligned} \quad (6)$$

В этом случае справедливо неравенство

$$\deg(\varphi) \leqslant 1 + (p-1) ill(\varphi) \ . \quad (7)$$

Отметим, что для булевых функций представление (6) рассматривалось в [7].

Представление отображений в виде разветвлений оказалось полезным при решении ряда криптографических задач.

4 Индекс гомоморфности и максимальный элемент таблицы разностей

Рассмотрим задачу о соотношении между $ih(\varphi)$ и $\mu l(\varphi)$. Ниже мы получаем оценки для $ih(\varphi)$ при заданном $\mu l(\varphi)$, и наоборот — оценки для $\mu l(\varphi)$ при заданном $ih(\varphi)$.

ТЕОРЕМА 2. *Если* $\varphi \in H^G$, *то*

$$\mu l(\varphi) \geqslant \frac{|G|}{ih(\varphi)} \ . \tag{8}$$

ДОКАЗАТЕЛЬСТВО. Пусть отображение $\varphi \in H^G$ представлено в виде гомоморфного разветвления (5), и мощность группы K минимальна, т. е. $|K| = ih(\varphi)$. В соответствии с равенством (3) каждое из разветвляемых отображений $\alpha_k \in RM_1$, $k \in K$, представим в виде

$$\alpha_k(x) = \lambda_k(x) + m_k \ , \tag{9}$$

где $k \in K$, $\lambda_k \in \mathrm{Hom}(G, H)$, $m_k \in H$, $k \in K$. Получим выражение для производной отображения φ по направлению $a \in G$:

$$\begin{aligned} \frac{d\,\varphi}{d\,a}(x) &= \varphi(x+a) - \varphi(x) = \alpha_{\rho(x+a)}(x+a) - \alpha_{\rho(x)}(x) = \\ &= \lambda_{\rho(x)+\rho(a)}(x) + \lambda_{\rho(x)+\rho(a)}(a) + m_{\rho(x)+\rho(a)} - \lambda_{\rho(x)}(x) - m_{\rho(x)} \ . \end{aligned} \tag{10}$$

Сначала рассмотрим случай, когда ядро гомоморфизма ρ нетривиально, т. е. $\mathrm{Ker}(\rho) \neq \{0\}$ и $|G| \underset{\neq}{>} |K|$. Пусть направление $a \in G\backslash\{0\}$ принадлежит ядру $\mathrm{Ker}(\rho)$, т. е. $\rho(a) = 0$. Тогда из (10) следует:

$$\frac{d\,\varphi}{d\,a}(x) = \lambda_{\rho(x)}(a) \ .$$

Для такого $a \in G\backslash\{0\}$, в частности, имеем

$$\mathrm{Ker}(\rho) \subseteq \left\{ x \in G \mid \frac{d\,\varphi}{d\,a}(x) = \lambda_0(a) \right\} \ .$$

Значит, для элемента $R^{\varphi}_{a,\lambda_0(a)}$ таблицы разностей справедливо неравенство:

$$R^{\varphi}_{a,\lambda_0(a)} \geqslant |\mathrm{Ker}(\rho)| \ . \tag{11}$$

Поскольку

$$|G| = |K| \cdot |\mathrm{Ker}(\rho)| = ih(\varphi) \cdot |\mathrm{Ker}(\rho)| \ , \tag{12}$$

то неравенство (11) эквивалентно неравенству

$$R^{\varphi}_{a,\lambda_0(a)} \geqslant \frac{|G|}{ih(\varphi)} \ .$$

Отсюда с учетом неравенства

$$\mu l(\varphi) \geqslant R^{\varphi}_{a,\lambda_0(a)}$$

следует неравенство (8).

В случае, когда ядро гомоморфизма ρ тривиально т. е. $\mathrm{Ker}(\rho) = \{0\}$ и $|G| = |K| = ih(\varphi)$, неравенство (8) становится очевидным. Теорема 2 доказана.

ЗАМЕЧАНИЕ. В случае булевых отображений теорема 2 доказана в работе [8].

Оценку (8) вообще говоря, нельзя улучшить, поскольку для $\varphi \in RM_1$ она достижима. Из теоремы 2 вытекает, что отображения с небольшими значениями $\mu l(\varphi)$ надо искать среди отображений с большими значениями $ih(\varphi)$.

ТЕОРЕМА 3. *Если группа гомоморфных трансляторов отображения $\varphi \in H^G$ тривиальна, то при любых $a \in G\backslash\{0\}$ и $b \in H$ справедливо неравенство*

$$R^{\varphi}_{a,b} \leqslant |G| - \frac{q-1}{q} \cdot \frac{|G|}{ih(\varphi)} \ , \tag{13}$$

где q — наименьший нетривиальный делитель числа $|G|/ih(\varphi)$.

ДОКАЗАТЕЛЬСТВО. По определению для любых $a \in G\backslash\{0\}$ и $b \in H$ элемент таблицы разностей $R^{\varphi}_{a,b}$ совпадает с числом решений относительно неизвестного $x \in G$ уравнения

$$\frac{d\,\varphi}{d\,a}(x) = b \ . \tag{14}$$

Пусть, как и при доказательстве теоремы 2, отображение $\varphi \in H^G$ представлено в виде гомоморфного разветвления (5), причем это представление выбрано таким образом, что мощность группы K минимальна, т. е. $|K| = ih(\varphi)$. Далее пусть каждое разветвляемое отображение $\alpha_k \in RM_1$, где $k \in K$ представлено в виде (9). Тогда производная отображения φ представляется в виде (10) и уравнение (14) принимает вид

$$\lambda_{\rho(x)+\rho(a)}(x) + \lambda_{\rho(x)+\rho(a)}(a) + m_{\rho(x)+\rho(a)} - \lambda_{\rho(x)}(x) - m_{\rho(x)} = b \ . \tag{15}$$

Положим $\rho(a) = r \in K$ и введем новый параметр $\rho(x) = k \in K$. Тогда рассматриваемое уравнение (14) эквивалентно объединению (в смысле объединения множества решений) следующих $|K|$ систем уравнений:

$$\begin{cases} (\lambda_{k+r} - \lambda_k)\,(x) = b + m_k - m_{k+r} - \lambda_{k+r}(a) \ , \\ \rho(x) = k \ . \end{cases} \tag{16}$$

Отметим, что систему уравнений (16) можно рассматривать как одно уравнение вида $\omega(x) = d$, где $\omega \in \mathrm{Hom}(A, B)$, $A = G \times G$, $B = H \times K$ и $d \in B$. Гомоморфизм ω совпадает с покоординатным действием пары гомоморфизмов $(\lambda_{k+r} - \lambda_k, \rho)$ на $G \times G$. В этом смысле систему уравнений (16) можно считать " неоднородной линейной". Значит, в случае совместности системы (16) все ее решения образуют некоторый смежный класс по подгруппе $\mathrm{Ker}(\rho) \bigcap \mathrm{Ker}(\lambda_{k+r} - \lambda_k)$.

Обозначим через $S(a,b)$ множество значений параметра $k \in K$, при которых система (16) совместна, а через $T_{k,a,b}$ число решений системы (16).

Поскольку при различных $k \in K$ множества решений систем (16) не пересекаются, то

$$R^{\varphi}_{a,b} = \sum T_{k,a,b} \ . \tag{17}$$

Для $T_{k,a,b}$ справедливо равенство:

$$T_{k,a,b} = \begin{cases} |\mathrm{Ker}(\rho) \bigcap \mathrm{Ker}(\lambda_{k+r} - \lambda_k)| \,, & \text{если } k \in S(a,b), \\ 0 & \text{в противном случае.} \end{cases}$$

Если $k \in S(a,b)$, то либо

$$\mathrm{Ker}(\rho) \subseteq \mathrm{Ker}(\lambda_{k+r} - \lambda_k)$$

и тогда $T_{k,a,b} = |\mathrm{Ker}(\rho)| = |G|/ih(\varphi)$, либо

$$\mathrm{Ker}(\rho) \not\subseteq \mathrm{Ker}(\lambda_{k+r} - \lambda_k)$$

и тогда $T_{k,a,b}$ не превосходит максимального порядка подгрупп группы $\mathrm{Ker}(\rho)$. Поэтому $T_{k,a,b} \leqslant \frac{1}{q} \cdot |G|/ih(\varphi)$, где q — наименьший нетривиальный делитель числа $|G|/ih(\varphi)$.

Теперь зафиксируем $a \in G \backslash \{0\}$, $b \in H$ и рассмотрим два случая.

1. $\mathrm{Ker}(\rho) \subseteq \mathrm{Ker}(\lambda_{k+r} - \lambda_k)$ для любого $k \in S(a,b)$. В силу равенства (17) в этом случае получаем

$$R^{\varphi}_{a,b} = |S(a,b)| \cdot \frac{|G|}{ih(\varphi)} \ .$$

Если $S(a,b) = K$, то $|S(a,b)| = ih(\varphi)$ и поэтому $R^{\varphi}_{a,b} = |G|$. Значит a — гомоморфный транслятор отображения φ.

Если же $S(a,b) \neq K$, то $|S(a,b)| \leqslant ih(\varphi) - 1$. Поэтому

$$R^{\varphi}_{a,b} \leqslant |G| - \frac{|G|}{ih(\varphi)} < |G| - \frac{q-1}{q} \cdot \frac{|G|}{ih(\varphi)} \ .$$

2. $\mathrm{Ker}(\rho) \not\subseteq \mathrm{Ker}(\lambda_{k'+r} - \lambda_{k'})$ при некотором $k' \in S(a,b)$. Тогда

$$T_{k',a,b} \leqslant \frac{1}{q} \cdot \frac{|G|}{ih(\varphi)} \ .$$

В этом случае число таких k из множества $S(a,b)$, что $T_{k,a,b} = |G|/ih(\varphi)$, не превосходит $ih(\varphi) - 1$. Поэтому

$$R^{\varphi}_{a,b} \leqslant (ih(\varphi) - 1) \cdot \frac{|G|}{ih(\varphi)} + \frac{1}{q} \cdot \frac{|G|}{ih(\varphi)} = |G| - \frac{q-1}{q} \cdot \frac{|G|}{ih(\varphi)} \ .$$

Таким образом, в любом случае либо отображение φ имеет нетривиальный гомоморфный транслятор, либо выполнено требуемое неравенство. Теорема 3 доказана.

Поскольку неравенство (13) справедливо при любых $a \in G \backslash \{0\}$ и $b \in H$, то аналогичная оценка справедлива и для $\mu l(\varphi)$:

СЛЕДСТВИЕ 1. *Если группа гомоморфных трансляторов отображения $\varphi \in H^G$ тривиальна, то*

$$\mu l(\varphi) \leqslant |G| - \frac{q-1}{q} \cdot \frac{|G|}{ih(\varphi)} \ , \tag{18}$$

где q — наименьший нетривиальный делитель числа $|G|/ih(\varphi)$.

В ряде частных случаев оценки (13) и (18) можно усилить. Для этого введем частный вид гомоморфных разветвлений. Будем считать, что в определении понятия разветвления группа K является элементарной абелевой 2-группой. Представление отображения $\varphi \in H^G$ в виде разветвления с таким дополнительным условием на группу K будем называть *2-разветвлением* отображения φ. Отметим, что в этом случае не всякое отображение $\varphi \in H^G$ для произвольных конечных абелевых групп H и G представимо в виде 2-разветвления. Аналогично индексу гомоморфности введем понятие индекса 2-гомоморфности: $ih_2(\varphi)$ — это минимальный порядок разветвляющей группы по всем возможным представлениям отображения φ в виде 2-разветвления (если индекс 2-гомоморфности определен, то он равен некоторой степени числа 2). Если для отображения φ определен параметр $ih_2(\varphi)$, то

$$ih(\varphi) \leqslant ih_2(\varphi) \ .$$

Отметим, что в случае, когда группа G является конечной абелевой 2-группой, понятия разветвления и 2-разветвления совпадают, так как любой гомоморфный образ элементарной абелевой 2-группы является элементарной абелевой 2-группой. В частности, в этом случае $ih(\varphi) = ih_2(\varphi)$.

ТЕОРЕМА 4. *Пусть для отображения $\varphi \in H^G$ определен индекс 2-гомоморфности. Если группа гомоморфных трансляторов отображения φ тривиальна, то при любых $a \in G \backslash \{0\}$ и $b \in H$ справедливо неравенство*

$$R^{\varphi}_{a,b} \leqslant |G| - \frac{|G|}{ih_2(\varphi)} \ .$$

ДОКАЗАТЕЛЬСТВО. Достаточно повторить доказательство теоремы 3, заменяя понятие гомоморфного разветвления и индекса гомоморфности на понятия 2-разветвления и индекса 2-гомоморфности соответственно. При этом отдельного рассмотрения требует только случай 2 из доказательства теоремы 3. Рассмотрим этот случай.

Если имеется k' из $S(a,b)$ такое, что $\mathrm{Ker}(\rho) \not\subseteq \mathrm{Ker}(\lambda_{k'+r} - \lambda_{k'})$, то

$$T_{k',a,b} \leqslant \frac{1}{q} \cdot \frac{|G|}{ih_2(\varphi)} \leqslant \frac{1}{2} \cdot \frac{|G|}{ih_2(\varphi)} \ ,$$

так как $q \geqslant 2$. Сначала рассмотрим случай когда $r = \rho(a) \neq 0$. В этом случае из (15) выберем две системы: при $k = k'$ и $k = k' + r$. При $k = k' + r$ возможны два случая: либо $k' + r \notin S(a,b)$ и тогда $T_{k'+r,a,b} = 0$, либо $k' + r \in S(a,b)$ и тогда $T_{k'+r,a,b} \leqslant \frac{1}{2} \cdot |G|/ih_2(\varphi)$, поскольку $\mathrm{Ker}(\rho) \not\subseteq \mathrm{Ker}(\lambda_{(k'+r)+r} - \lambda_{k'+r}) = \mathrm{Ker}(\lambda_{k'+r} - \lambda_{k'})$. Значит, $T_{k,a,b} \neq |G|/ih_2(\varphi)$ как при $k = k'$, так и при $k = k' + r$. Поэтому число таких k из множества $S(a,b)$, что $T_{k,a,b} = |G|/ih_2(\varphi)$, не превосходит $ih_2(\varphi) - 2$. Поэтому

$$R^{\varphi}_{a,b} \leqslant (ih_2(\varphi) - 2) \cdot \frac{|G|}{ih_2(\varphi)} + 2 \cdot \frac{1}{2} \cdot \frac{|G|}{ih_2(\varphi)} = |G| - \frac{|G|}{ih_2(\varphi)} \ .$$

В случае, когда $r = \rho(a) = 0$, система уравнений (16) относительно неизвестного $x \in G$ принимает вид

$$\begin{cases} b = \lambda_k(a) \ , \\ \rho(x) = k \ . \end{cases} \tag{19}$$

Если $b = \lambda_k(a)$, то система (19) имеет $|\mathrm{Ker}\,(\rho)| = |G|/ih_2(\varphi)$ решений. Если же $b \neq \lambda_k(a)$, то система (19) не имеет решений. В случае, когда при любом $k \in K$ все элементы $\lambda_k(a)$ совпадают, имеем $R^{\varphi}_{a,\lambda_k(a)} = |G|$, т. е. a является гомоморфным транслятором. В случае, когда не все элементы $\lambda_k(a)$ совпадают, имеем

$$R^{\varphi}_{a,b} \leqslant (ih_2(\varphi) - 1)\,\frac{|G|}{ih_2(\varphi)} = |G| - \frac{|G|}{ih_2(\varphi)} \ .$$

Теорема 4 доказана.

СЛЕДСТВИЕ 2. *Пусть для отображения $\varphi \in H^G$ определен индекс 2-гомоморфности. Если группа гомоморфных трансляторов отображения φ тривиальна, то*

$$\mu l(\varphi) \leqslant |G| - \frac{|G|}{ih_2(\varphi)} \ .$$

СЛЕДСТВИЕ 3. *Если G — элементарная абелева 2-группа и группа гомоморфных трансляторов отображения $\varphi \in H^G$ тривиальна, то*

$$\mu l(\varphi) \leqslant |G| - \frac{|G|}{ih(\varphi)} \ .$$

Объединяя оценки (8) и (18), в случае тривиальности группы гомоморфных трансляторов мы получаем двухстороннюю оценку максимального элемента таблицы разностей при известном индексе гомоморфности:

$$|G| - \frac{q-1}{q} \cdot \frac{|G|}{ih(\varphi)} \geqslant \mu l(\varphi) \geqslant \frac{|G|}{ih(\varphi)} \ .$$

Если G — элементарная абелева 2-группа, двусторонняя оценка принимает вид:

$$|G| - \frac{|G|}{ih(\varphi)} \geqslant \mu l(\varphi) \geqslant \frac{|G|}{ih(\varphi)} \ .$$

Из последнего неравенства следует, что если $ih(\varphi) = 2$, то $\mu l(\varphi) = |G|/2$ (так как группа порядка 2 является элементарной абелевой 2-группой). Таким образом, справедливо

СЛЕДСТВИЕ 4. *Если группа гомоморфных трансляторов отображения $\varphi \in H^G$ тривиальна и индекс гомоморфности равен 2, т. е. $ih(\varphi) = 2$, то*

$$\mu l(\varphi) = \frac{|G|}{2} \ .$$

Доказанные неравенства позволяют получить следующее неравенство для индекса гомоморфности $ih(\varphi)$ при известном μl:

$$ih(\varphi) \geqslant \max\left\{ \frac{|G|}{\mu l(\varphi)},\ \frac{q-1}{q} \cdot \frac{|G|}{|G| - \mu l(\varphi)} \right\} \ .$$

Если G — элементарная абелева 2-группа, то последняя оценка принимает вид:

$$ih(\varphi) \geqslant \max\left\{\frac{|G|}{\mu l(\varphi)},\ \frac{|G|}{|G| - \mu l(\varphi)}\right\} .$$

Отметим, что приведенные конструкции позволяют улучшить оценки в частных случаях. Например, можно вводить новые частные виды разветвлений отображений, накладывая другие дополнительные условия на группу K. При этом пока остается нерешенной задача получения необходимых и достаточных условий представимости отображения в виде таких разветвлений частного вида.

В практике криптографических исследований *a priori* задано отображение не групп, а отображение конечных множеств (см., например, [9, 10]). Только в ходе исследований эти множества наделяются той или иной групповой структурой. Очевидно, что эффективность применяемых методов может существенно зависеть от того, какие групповые структуры при этом будут введены. Поэтому в связи с установленными фактами интересно рассмотреть следующую задачу. Пусть задано отображение $\varphi : \mathcal{G} \to \mathcal{H}$, где $\mathcal{G}$ и $\mathcal{H}$ — произвольные конечные множества. На множествах $\mathcal{G}$ и $\mathcal{H}$ требуется ввести такие структуры конечных (абелевых) групп, чтобы максимальный элемент таблицы разностей отображения φ оказался максимальным (т. е. чтобы после введения структуры групп эффективность метода дифференциального криптоанализа повысилась). Не менее интересно (и важно для криптографических приложений) оценить этот максимум.

ЛИТЕРАТУРА

1. БЕРМАН С. Д. К теории групповых кодов// Кибернетика. 1967. № 1. С. 31–39.

2. ЛЕНГ С. Алгебра. М.: Мир, 1968.

3. ЛОГАЧЕВ О. А., САЛЬНИКОВ А. А., ЯЩЕНКО В. В. Бент-функции на конечной абелевой группе// Дискретная математика. 1997. Т. **9**, вып. 4. С. 3–20.

4. ЛОГАЧЕВ О. А., ЯЩЕНКО В. В. Коды типа Рида-Маллера на конечной абелевой группе// Проблемы передачи информации. 1998. Т. **34**, вып. 2. С. 32–46.

5. ЛОГАЧЕВ О. А., САЛЬНИКОВ А. А., ЯЩЕНКО В. В. Невырожденная нормальная форма булевых функций// Докл. РАН. 2000. Т. **373**, № 2. С. 164–167.

6. ЯЩЕНКО В. В. Свойства булевых отображений, сводимые к свойствам их координатных функций// Вестник МГУ. Сер. Математика. Механика. 1997. № 4. С. 11–13.

7. ЯЩЕНКО В. В. О критерии распространения для булевых функций и о бент-функциях// Проблемы передачи информации. 1997. Т. **33**, вып. 1. С. 75–86.

8. ЯЩЕНКО В. В. О двух характеристиках нелинейности булевых отображений// Дискретный анализ и исследование операций. Сер. 1. 1998. Т. **5**, № 2. С. 90–96.

9. BIHAM E., SHAMIR A. Differential cryptanalysis of DES-like cryptosystems// *Advances in Cryptology. Proceedings of CRYPTO'90.* (Lecture Notes in Comput. Sci., V. **537**), Berlin: Springer-Verlag, 1991. P. 2–21.

10. EVERTSE J.-H. Linear structures in blockciphers// *Advances in Cryptology — EUROCRYPT'87.* (Lecture Notes in Comput. Sci., V. **304**), Berlin: Springer-Verlag, 1988. P. 249–266.

11. ROTHAUS O. S. On "Bent" functions// J. of Combinatorial Theory. Ser. A, 1976. V. **20**, № 3, P. 300–305.

Адрес авторов:
МГУ, Воробьевы горы,
119899, Москва, Россия

Статья поступила
июль 2000 г.