Оценки некоторых параметров отображений конечных абелевых групп

О.А. Логачев, А.А. Сальников, В.В. Ященко

Москва

Объектом нашего исследования являются отображения конечной абелевой группы N в конечную абелеву группу M: $M^N = \{\varphi : N \to M\}$; $\mathrm{Hom}(N, M)$ — множество гомоморфизмов из N в M. Множество M^N является конечной абелевой группой относительно операции поточечного сложения отображений.

Мы активно используем понятие производной отображения $\varphi \in M^N$ по направлению $a \in N$:

$$\frac{d\,\varphi}{d\,a}(n) = \varphi(n+a) - \varphi(n), \quad \forall n \in N \ .$$

Понятие производной позволяет индуктивным образом ввести вложенную систему подгрупп в группе всех отображений M^N: $RM_{-1}(N, M) = \{\varphi \in M^N \mid \varphi(n) = 0,\ \forall n \in N\}$. Далее семейства отображений определяются с помощью индуктивного шага:

$$RM_j(N, M) = \left\{ \varphi \in M^N \mid \frac{d\,\varphi}{d\,a} \in RM_{j-1}(N, M),\ \forall a \in N \right\},\ j = 0, 1, 2, \ldots$$

Множества $RM_j(N, M)$ образуют вложенную систему подгрупп в группе M^N:

$$RM_{-1} \subseteq RM_0 \subseteq \ldots \subseteq RM_j \subseteq RM_{j+1} \ldots$$

При изучении отображений $\varphi \in M^N$ важную роль играют следующие подмножества группы N:

$$L^j_\varphi = \left\{ a \in N \mid \frac{d\,\varphi}{d\,a} \in RM_j \right\}, \quad j = -1, 0, 1, 2, \ldots$$

Множества L^j_φ образуют вложенную систему подгрупп в группе N:

$$L^{-1}_\varphi \subseteq L^0_\varphi \subseteq \ldots \subseteq L^j_\varphi \subseteq L^{j+1}_\varphi \ldots$$

Веса всех производных отображения $\varphi \in M^N$ по ненулевым направлениям можно расположить в виде таблицы R^φ из $|N|-1$ строк и $|M|$ столбцов — строку с номером $a \in N\backslash\{0\}$ таблицы R^φ составляют элементы веса отображения $\frac{d\,\varphi}{d\,a}$, т.е.

$$R^\varphi_{a,b} = \left| \left(\frac{d\,\varphi}{d\,a} \right)^{-1} (b) \right|, \quad \forall a \in N\backslash\{0\}, b \in M \ .$$

Элементы таблицы R^φ связаны определенными соотношениями. В частности, очевидно, что для любого $a \in N$ имеет место равенство

$$\sum_{b \in M} R^\varphi_{a,b} = |N| \ . \tag{1}$$

Таблица R^φ имеет многочисленные приложения в дифференциальном (разностном) криптоанализе (см. [3]). При оценке эффективности дифференциального метода криптографического анализа используется максимальный элемент таблицы разностей

$$\mu l(\varphi) = \max_{\substack{a \in N\backslash\{0\} \\ b \in M}} R^\varphi_{a,b} \ .$$

В силу равенства (1) очевидно, что для любого отображения $\varphi \in M^N$ выполнено неравенство $\mu l(\varphi) \geqslant \frac{|N|}{|M|}$.

Теорема 1. *Для произвольного отображения $\varphi \in M^N$ имеет место оценка*

$$\mu l(\varphi) \geqslant \max \left\{ |L^0_\varphi|, \frac{|N|}{|M|} \right\} \ .$$

Приведем одно обобщение введенного в работе [1] понятия гомоморфного разветвления отображений.

Определение 1. Пусть кроме групп N и M задана еще одна конечная абелева группа K. Пусть также заданы $\rho \in \mathrm{Hom}(N,K)$ и семейство отображений (не обязательно различных) $\{\, \alpha_k \in RM_t(N,M) \mid k \in K \,\}$, заиндексированных элементами группы K. Отображение $\varphi \in M^N$ определим равенством

$$\varphi(n) = \alpha_{\rho(n)}(n) \ . \tag{2}$$

Будем говорить, что φ — гомоморфное разветвление степени t с разветвляющей группой K и разветвляющим отображением ρ. При этом отображения $\alpha_k \in RM_t(N,M)$, $k \in K$ будем называть разветвляемыми.

В работе [1] рассмотрен случай $t = 1$. Любое отображение $\varphi \in M^N$ можно представить в виде гомоморфного разветвления степени t для любого t. Будем считать, что гомоморфизм ρ сюръективен.

Представления отображений в виде гомоморфных разветвлений не однозначно. Минимальный порядок разветвляющей группы по всем возможным представлениям отображения $\varphi \in M^N$ в виде гомоморфного разветвления степени t назовем индексом гомоморфности степени t отображения φ и будем обозначать символом $ih_t(\varphi)$, а такое разветвление будем называть минимальным разветвлением степени t.

Из введенного определения очевидно, что если $t_1 \leqslant t_2$, то для любого отображения $\varphi \in M^N$ имеет место неравенство $ih_{t_1}(\varphi) \geqslant ih_{t_2}(\varphi)$. Кроме того, равенство $ih_t(\varphi) = 1$ выполнено тогда и только тогда, когда $\varphi \in RM_t$.

Лемма 1. *Пусть отображение $\varphi \in M^N$ имеет вид*

$$\varphi(n) = \lambda(n) + \psi(n), \quad n \in N \ ,$$

где $\lambda \in RM_t$. Тогда, имеет место равенство

$$ih_t(\varphi) = ih_t(\psi) \ .$$

Доказанные в[2] результаты позволяют дать верхнюю оценку для индекса гомоморфности через порядки групп L^t_φ.

Теорема 2. *Для любого отображения $\varphi \in M^N$ имеет место неравенство*

$$ih_t(\varphi) \leqslant \frac{|N|}{|L^t_\varphi|} \ .$$

Работа поддержана Российским фондом фундаментальных исследований (номера проектов 99-01-00929 и 99-01-00941).

Литература

[1] Логачев О.А., Сальников А.А., Ященко В.В. Некоторые характеристики нелинейности групповых отображений. *Дискретный анализ и исследование операций*, в печати.

[2] Логачев О. А., Сальников А. А., Ященко В. В. *Нормальная форма отображений конечных абелевых групп.* тезисы доклада на седьмом международном семинаре "Дискретная математика и ее приложения", 2001, Москва, 29 января — 2 февраля, Московский государственный университет им. М.В.Ломоносова.

[3] E. Biham, A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, *Advances in Cryptology, Proceedings of CRYPTO'90, Lecture Notes in Computer Science*, **537**, Springer-Verlag, 1991, 2–21.