Нормальная форма отображений конечных абелевых групп

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

Москва

Пусть N и M — конечные абелевы группы. Множество всех отображений группы N в группу M будем обозначать $M^N = \{\, \varphi : N \to M \,\}$; $\mathrm{Hom}(N, M)$ — множество гомоморфизмов из N в M. Множество M^N является конечной абелевой группой относительно операции поточечного сложения отображений.

Определение 1. Производной отображения $\varphi \in M^N$ по направлению $a \in N$ называется следующее отображение $\dfrac{d\,\varphi}{d\,a} \in M^N$:

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

Производная по нулевому направлению является отображением, тождественно равным нулю.

Понятие производной позволяет индуктивным образом ввести вложенную систему подгрупп в группе всех отображений M^N. Первым шагом в такой конструкции является отображение, тождественно равное нулю на 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:

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

Легко проверить, что RM_0 — это отображения-константы, а RM_1 — это гомоморфизмы и их сдвиги.

Существуют пары групп N и M такие, что не всякое отображение из M^N лежит в некотором семействе RM_j. Если же для отображения $\varphi \in M^N$ существует номер j такой, что $\varphi \in RM_j$, то корректно определен следующий параметр, называемый степенью нелинейности отображения φ:

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

Если $\varphi \notin RM_j$ для любого j, то положим $\deg(\varphi) = \infty$.

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

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

Множества L_φ^j образуют вложенную систему подгрупп в группе N:

$$L_\varphi^{-1} \subseteq L_\varphi^0 \subseteq \ldots \subseteq L_\varphi^j \subseteq L_\varphi^{j+1} \ldots$$

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. 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 $\mu l(\varphi) \geqslant \frac{|N|}{|M|}$.

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

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 предыдущем разделе результаты позволяют дать верхнюю оценку для индекса гомоморфности через порядки групп L^t_φ.

Теорема 1. *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. *Невырожденная нормальная форма булевых функции.* Доклады Академии наук, 2000, **373**, № 2, стр. 164–167.