УДК 519.719.325

# К ОПРЕДЕЛЕНИЮ СТЕПЕНИ НЕЛИНЕЙНОСТИ ДИСКРЕТНОЙ ФУНКЦИИ НА ЦИКЛИЧЕСКОЙ ГРУППЕ[1]

А. В. Черемушкин

Предлагается аддитивный подход к определению степени нелинейности дискретных функций, заданных на циклической группе. Показано, что степень нелинейности конечна, если и только если порядок группы есть степень простого числа; найдены верхние оценки степени нелинейности. Показано, что для полиномиальных функций над кольцом $\mathbb{Z}_{p^n}$ степень нелинейности функции совпадает с минимальной степенью многочлена, задающего эту функцию.

**Ключевые слова:** *дискретные функции, степень нелинейности.*

В работе [1] предложен аддитивный подход к определению степени нелинейности функции на основе свойств конечных производных. Его суть заключается в следующем. Для функций $F : G \to H$, у которых на множествах $G$ и $H$ заданы структуры абелевых групп, *производная по направлению* $\Delta_a F$, $a \in G$, функции $F$ определяется равенствами

$$\Delta_a F(x) = F(x + a) - F(x),$$

где $x \in G$. *Степенью нелинейности* функции $F : G \to H$ (обозначается $\mathrm{dl}\, F$) называется минимальное натуральное число $m$, такое, что

$$\Delta_{a_1} \dots \Delta_{a_{m+1}} F(x) = 0$$

при всех $a_1, \dots, a_{m+1}, x \in G$. Если такого числа $m$ не существует, то полагаем $\mathrm{dl}\, F = \infty$.

В случае элементарных абелевых $p$-групп степень нелинейности функции $p^n$-значной логики полностью определяется свойствами операции сложения. Поэтому при любом способе задания на этой группе операции умножения так, чтобы в результате получилось поле из $p^n$ элементов, степень нелинейности функций инвариантна по отношению к выбору операции умножения.

В случае произвольных абелевых групп вопрос о свойствах параметра $\mathrm{dl}\, F$ остается открытым. В данной работе изучается случай циклических групп.

Показано, что параметр $\mathrm{dl}\, F$ в случае, когда на множестве аргументов и значений заданы структуры циклических групп, может принимать конечные значения, только когда порядки групп являются примарными числами.

**Теорема 1.** Если $F : G^m \to H$, где $G$ и $H$ — циклические группы порядков $g \geqslant 2$ и $h \geqslant 2$ соответственно, причем $\mathrm{dl}\, F < \infty$, то при некотором простом $p \geqslant 2$ выполнены равенства $g = p^n$ и $h = p^k$ при некоторых $n \geqslant 1$ и $k \geqslant 1$.

Следующая теорема показывает, что введенное выше «аддитивное» определение степени нелинейности корректно и параметр $\mathrm{dl}\, F$ принимает конечное значение для любой функции, заданной на циклических группах примарного порядка.

**Теорема 2.** Если $F : G^m \to H^t$, $G = \mathbb{Z}_{p^n}$, $H = \mathbb{Z}_{p^k}$, $p > 2$, $n \geqslant 1$, $k \geqslant 1$, $m \geqslant 1$, $t \geqslant 1$, и $F = (F_1, \dots, F_t)$, где $F_i : G^m \to H$, $1 \leqslant i \leqslant t$, — соответствующие координатные функции, то

$$\mathrm{dl}\, F = \max\{\mathrm{dl}\, F_i \ : \ 1 \leqslant i \leqslant t\} \leqslant m(p^n - (k-1)(p-1)p^{n-1} - 1).$$

[1]Работа выполнена при поддержке гранта Президента РФ НШ № 6260.2012.10.

Преимущество данного подхода к определению степени нелинейности заключается в том, что он полостью определяется свойствами только операции сложения. Вместе с тем в случае циклических групп, в отличие от элементарных абелевых групп, вопрос о способе выбора операции умножения представляется не таким однозначным. Если естественным образом рассматривать циклические группы примарного порядка как аддитивные группы колец вычетов с имеющимися в них операциями умножения, то определение степени нелинейности через степень многочлена является неудобным, так как не всякая функция $F$ может быть задана многочленом (или набором многочленов координатных функций). Полиномиальные функции над кольцом вычетов, то есть функции, которые могут быть заданы многочленом над этим кольцом, составляют относительно малую долю функций [2, 3]. Следует отметить, что для полиномиальных функций над кольцом $\mathbb{Z}_{p^n}$ степень нелинейности функции совпадает с минимальной степенью многочлена, задающего эту функцию.

**Теорема 3.** Если $F : G^m \to G$ — полиномиальная функция над кольцом $G = \mathbb{Z}_{p^n}$, $p > 2$, $n \geqslant 1$, $m \geqslant 1$, и $P(x_1, \dots x_n) \in \mathbb{Z}_{p^n}[x_1, \dots x_n]$ — многочлен минимальной степени, задающий эту функцию, то степень нелинейности совпадает со степенью многочлена $P(x_1, \dots x_n)$:

$$\mathrm{dl}\, F = \deg P.$$

Из определения степени нелинейности с очевидностью вытекает

**Теорема 4.** Если $G$ и $H$ — циклические $p$-группы примарного порядка и $R$ — подгруппа в $G$, то для степеней нелинейности функции $F : G \to H$ и её ограничения на подгруппу $R$, $F|_R : R \to H$, выполнено неравенство $\mathrm{dl}\,(F|_R) \leqslant \mathrm{dl}\, F$.

Подробное изложение представленных результатов можно найти в [4].

ЛИТЕРАТУРА

1. *Черемушкин А. В.* Аддитивный подход к определению степени нелинейности дискретной функции // Прикладная дискретная математика. 2010. № 2(8). С. 22–33.
2. *Keller G. and Olson F.* Counting polynomial functions (mod $p^n$) // Duke Math. J. 1968. V. 35. P. 835–838.
3. *Chen Z.* On polynomial functions from $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \mathbb{Z}_{n_r}$ to $\mathbb{Z}_m$ // Discrete Math. 1996. V. 162. P. 67–76.
4. *Черемушкин А. В.* Аддитивный подход к определению степени нелинейности дискретной функции на циклической группе примарного порядка // Прикладная дискретная математика. 2013. № 2(20). С. 26–38.

УДК 621.391: 519.728

## ЭКОНОМНОЕ ПРЕДСТАВЛЕНИЕ НЕДООПРЕДЕЛЁННЫХ ДАННЫХ И ДИЗЪЮНКТИВНЫЕ КОДЫ[1]

Л. А. Шоломов

Предложены экономные представления недоопределённых данных, позволяющие полностью восстанавливать исходные данные. Установлена их связь с дизъюнктивными кодами, получены оценки длины представлений.

**Ключевые слова:** *представление недоопределённых данных, дизъюнктивный код, свободная от покрытий матрица.*

[1]Работа поддержана ОНИТ РАН по программе фундаментальных исследований.