УДК 519.719.325

О ЧИСЛЕ ДИСКРЕТНЫХ ФУНКЦИЙ НА ЦИКЛИЧЕСКОЙ ГРУППЕ ПРИМАРНОГО ПОРЯДКА С ЗАДАННОЙ СТЕПЕНЬЮ НЕЛИНЕЙНОСТИ

А. В. Черемушкин

Предлагается способ вычисления степени нелинейности дискретных функций, заданных на циклической группе примарного порядка, основанный на свойствах разложения Ньютона. Найдены значения степени нелинейности для базисных функций этого разложения. Для циклических групп порядков p^2 и p^3 приводится распределение числа функций с заданным значением степени нелинейности.

Ключевые слова: *дискретные функции, степень нелинейности.*

Напомним определения из работы [1]. Будем рассматривать функции $F : G^m \to H$, где G и H — циклические группы. Считаем, что циклические группы — это аддитивные группы колец вычетов. *Степенью нелинейности* функции F (обозначается $\mathrm{dl}\, F$) называется минимальное натуральное число t, такое, что $\Delta_{a_1} \dots \Delta_{a_{t+1}} F(x) = 0$ при всех $a_1, \dots, a_{t+1}, x \in G^m$, где $\Delta_a F(x) = F(x+a) - F(x)$, $a, x \in G^m$. Пусть D_t — множество функций со степенью нелинейности t.

Предлагается подход к описанию классов D_t на основе разложения Ньютона. Теорема 1 даёт точные значения степени нелинейности для базисных функций этого разложения.

Лемма 1. Пусть $n \geqslant 2$, p простое и $1 \leqslant i \leqslant p^n - 1$. Тогда значения производных функции $F_i(x) = \binom{x}{i} \bmod p^n$ при $1 \leqslant x \leqslant p^n - 1$ удовлетворяют равенствам

$$\Delta_1 \binom{x}{i} \equiv \begin{cases} \binom{x}{i-1} \pmod{p^n}, & \text{если } (p^n, i) = 1, \\ \binom{x}{i-1} - \binom{p^n}{i}\binom{x}{p^n-1} \pmod{p^n}, & \text{если } (p^n, i) \neq 1. \end{cases}$$

Теорема 1. Пусть $n \geqslant 1$ и p простое. Тогда степень нелинейности функции $F_i(x) = \binom{x}{i} \bmod p^n$, $1 \leqslant i \leqslant p^n - 1$, равна

$$\mathrm{dl}\, F_i = \begin{cases} i + (t-1)(p-1)p^{n-1} + p^n - p^t, & \text{если } p^t \leqslant i \leqslant p^{t+1} - 1,\ 1 \leqslant t \leqslant n-1, \\ i, & \text{если } 1 \leqslant i \leqslant p-1. \end{cases}$$

Следствие 1. В условиях теоремы 1 выполняются равенства

$$\mathrm{dl}\, F_i - \mathrm{dl}\, F_{i-1} = \begin{cases} (p-1)p^{n-1} + p^t - p^{t+1}, & \text{если } i = p^t, \quad 1 \leqslant t \leqslant n-1, \\ 1, & \text{если } i \neq p^t, \quad 1 \leqslant t \leqslant n-1. \end{cases}$$

Следствие 2. Пусть $m \geqslant 2$, $n \geqslant 1$, $p \geqslant 2$ и разложение функции $F : \mathbb{Z}_{p^n}^m \to \mathbb{Z}_{p^n}$ имеет вид

$$F(x_1, \dots, x_m) = \sum_{i_1, \dots, i_m = 0}^{n-1} h(i_1, \dots, i_m) \binom{x_1}{i_1} \cdots \binom{x_m}{i_m} \bmod p^n.$$

Тогда следующие условия эквивалентны:

1) функция F имеет максимальную степень нелинейности, равную

$$\mathrm{dl}F = m(p^n + (k-1)(p-1)p^{n-1} - 1);$$

2) коэффициент $h(p^n - 1, \ldots, p^n - 1)$ обратим в кольце $\mathbb{Z}_{p^n}$, т. е.

$$(h(p^n - 1, \ldots, p^n - 1), p) = 1;$$

3) сумма значений функции F является обратимым элементом в кольце $\mathbb{Z}_{p^n}$:

$$\left(\sum_{x_1,\ldots,x_m} F(x_1, \ldots, x_m) \bmod p^n,\, p \right) = 1.$$

Данный подход позволяет подсчитать число функций малой и близкой к максимальной степени нелинейности, а также найти точное распределение числа функций с заданным значением степени нелинейности для циклических групп порядков p^2 и p^3.

Теорема 2. Пусть $p \geqslant 2$. Тогда число функций степени нелинейности i среди функций вида $F : G \to H$, $G = H = \mathbb{Z}_{p^2}$, равно

$$|D_i| = \begin{cases} 1, & \text{если } i = -1, \\ p^{2i}(p^2 - 1), & \text{если } 0 \leqslant i \leqslant p - 1, \\ p^{i+p}(p - 1), & \text{если } p \leqslant i \leqslant p^2 + (p-1)p - 1. \end{cases}$$

Теорема 3. Пусть $p \geqslant 2$. Тогда число функций степени нелинейности i среди функций вида $F : G \to H$, $G = H = \mathbb{Z}_{p^3}$, равно

$$|D_i| = \begin{cases} 1, & \text{если } i = -1, \\ p^{3i}(p^3 - 1), & \text{если } 0 \leqslant i \leqslant p - 1, \\ p^{2i+p}(p^2 - 1), & \text{если } p \leqslant i \leqslant p^2 - 1, \\ p^{i+p^2+p}(p - 1), & \text{если } p^2 \leqslant i \leqslant p^3 - 1, \\ p^{2i-p^3+p^2+p}(p^2 - 1), & \text{если } p^3 \leqslant i \leqslant p^3 + p^2 - p - 1, \\ p^{i+2p^2}(p - 1), & \text{если } p^3 + p^2 - p \leqslant i \leqslant p^3 + 2(p-1)p^2 - 1. \end{cases}$$

Подробное изложение представленных результатов можно найти в [2].

ЛИТЕРАТУРА

1. *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.
2. *Черемушкин А. В.* Вычисление степени нелинейности функции на циклической группе примарного порядка // Прикладная дискретная математика. 2014. № 2(24). С. 37–47.