2013 Теоретические основы прикладной дискретной математики №2(20)

DOI 10.17223/20710410/20/4

УДК 519.719.325

АДДИТИВНЫЙ ПОДХОД К ОПРЕДЕЛЕНИЮ СТЕПЕНИ НЕЛИНЕЙНОСТИ ДИСКРЕТНОЙ ФУНКЦИИ НА ЦИКЛИЧЕСКОЙ ГРУППЕ ПРИМАРНОГО ПОРЯДКА[1]

А. В. Черемушкин

Институт криптографии связи и информатики, г. Москва, Россия

E-mail: avc238@mail.ru

Предлагается подход к определению степени нелинейности дискретных функций, заданных на циклической группе примарного порядка. 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.*

Введение

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 [1] показано, что 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 dl может принимать конечное значение только в случае, когда циклические группы являются p-группами при некотором $p \geqslant 2$ (теорема 1). Для случая примарных циклических групп найдены верхние оценки степени нелинейности (теоремы 2 и 3) и показано, что для полиномиальных функций над кольцом $\mathbb{Z}_{p^n}$ степень нелинейности функции совпадает с минимальной степенью многочлена, задающего эту функцию (теорема 6).

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

1. Вспомогательные утверждения

В дальнейшем потребуются следующие свойства биномиальных коэффициентов.

Лемма 1. Пусть $\nu_p\{k\}$ — максимальная степень числа p, делящая число k. Тогда при $1 \leqslant k \leqslant p^n$ справедливо равенство

$$\nu_p\left\{\binom{p^n}{k}\right\} = n - \nu_p\{k\}.$$

Доказательство. Рассмотрим числитель и знаменатель выражения для $\binom{p^n}{k}$:

$$\binom{p^n}{k} = \frac{p^n(p^n-1)\cdot\ldots\cdot(p^n-k+1)}{1\cdot 2\cdot\ldots\cdot k}.$$

Нетрудно видеть, что при $1 \leqslant i \leqslant k-1$ выполнено равенство $\nu_p\{p^n - i\} = \nu_p\{i\}$. Поэтому $\nu_p\left\{\binom{p^n}{k}\right\} = \nu_p\left\{\frac{p^n}{k}\right\} = \nu_p\{n\} - \nu_p\{k\} = n - \nu_p\{k\}$. ■

В частности, минимальное значение при $1 \leqslant k \leqslant p^n - 1$ достигается для $k = ip^{n-1}$, $1 \leqslant i \leqslant p-1$, и равно

$$\nu_p\left\{\binom{p^n}{ip^{n-1}}\right\} = \nu_p\left\{\binom{p^n}{p^{n-1}}\right\} = 1.$$

Лемма 2. При всех $2 \leqslant k \leqslant n$ и $1 \leqslant i \leqslant p-1$ справедливо равенство

$$\binom{p^k}{ip^{k-1}} \equiv \binom{p^{k-1}}{ip^{k-2}} \pmod{p^k}.$$

Доказательство. Имеем

$$\binom{p^k}{ip^{k-1}} \equiv \frac{p^k(p^k-1)\cdot\ldots\cdot(p^k-pa)\cdot\ldots\cdot(p^k-ip^{k-1}+1)}{1\cdot 2\cdot\ldots\cdot pa\cdot\ldots\cdot(ip^{k-1}-1)ip^{k-1}} \equiv$$
$$\equiv \frac{p(p^k-1)(p^k-2)\cdot\ldots\cdot(p^{k-1}-a)\cdot\ldots\cdot(p^k-ip^{k-1}+1)}{1\cdot 2\cdot\ldots\cdot a\cdot\ldots\cdot(ip^{k-1}-1)i} \pmod{p^k}.$$

Заметим, что в знаменателе все сомножители, не кратные p, являются обратимыми элементами кольца $\mathbb{Z}_{p^n}$. Каждому сомножителю вида pa соответствует в числителе сомножитель вида $p^k - pa$, $1 \leqslant a < ip^{k-1} - 1$. Всего сомножителей, кратных p, ровно ip^{k-2}.

Представим теперь последнюю дробь в виде произведения двух сомножителей, в первый из которых включим все сомножители числителя и знаменателя, взаимно простые с p, а во второй — все кратные p, разделив каждый из них на p:

$$\frac{(p^k-1)(p^k-2)\cdot\ldots\cdot(p^k-ip^{k-1}+1)}{1\cdot 2\cdot\ldots\cdot(ip^{k-1}-1)} \cdot \frac{p^{k-1}(p^{k-1}-1)\cdot\ldots\cdot(p^{k-1}-ip^{k-2}+1)}{1\cdot 2\cdot\ldots\cdot(ip^{k-2}-1)ip^{k-2}}.$$

Осталось заметить, что для каждого j, лежащего в интервале $1 \leqslant j \leqslant ip^{k-1}-1$ и взаимно простого с p, выполняется сравнение

$$\frac{p^k-j}{j} \equiv \frac{-j}{j} \equiv -1 \pmod{p^k}.$$

Таким образом,

$$\binom{p^k}{ip^{k-1}} \equiv \frac{(-1)(-2)\cdot\ldots\cdot(-ip^{k-1}+1)}{1\cdot 2\cdot\ldots\cdot(ip^{k-1}-1)}\binom{p^{k-1}}{ip^{k-2}} \equiv (-1)^{ip^{k-1}-ip^{k-2}}\binom{p^{k-1}}{ip^{k-2}} \pmod{p^k}.$$

При $p>2$ или при $p=2$ и $k>2$ число $ip^{k-1}-ip^{k-2}=ip^{k-2}(p-1)$ является чётным. При $p=k=2$ имеем $\binom{4}{2}\equiv\binom{2}{1} \pmod{2^2}$. ■

Следствие 1. При всех $2\leqslant k\leqslant n$ и $1\leqslant i\leqslant p-1$ справедливы сравнения

$$\binom{p^k}{ip^{k-1}} \equiv \binom{p^{k-j}}{ip^{k-j-1}} \pmod{p^{k-j}}, \quad 1\leqslant j\leqslant k-1,$$

в частности,

$$\binom{p^n}{ip^{n-1}} \equiv \binom{p}{i} \pmod{p}.$$

Доказательство. Достаточно показать, что при $3\leqslant k\leqslant n$ выполнено сравнение

$$\binom{p^k}{ip^{k-1}} \equiv \binom{p^{k-2}}{ip^{k-3}} \pmod{p^{k-1}}.$$

Имеем

$$\binom{p^k}{ip^{k-1}} \equiv \binom{p^{k-1}}{ip^{k-2}} \pmod{p^k},$$

$$\binom{p^{k-1}}{ip^{k-2}} \equiv \binom{p^{k-2}}{ip^{k-3}} \pmod{p^{k-1}}.$$

Осталось заметить, что если $a\equiv b \pmod{p^k}$, то $a\equiv b \pmod{p^{k-1}}$. ■

Аналогично лемме 2 доказывается

Лемма 3. При $1\leqslant k\leqslant n$, $1\leqslant r\leqslant p-1$ и $1\leqslant i\leqslant p-1$ справедливо равенство

$$\binom{p^k-rp^{k-1}}{ip^{k-1}} \equiv \binom{p^{k-1}-rp^{k-2}}{ip^{k-2}} \pmod{p^k}.$$

Следствие 2. При всех $2\leqslant k\leqslant n$, $1\leqslant r\leqslant p-1$ и $1\leqslant i\leqslant p-1$ справедливы сравнения

$$\binom{p^k-rp^{k-1}}{ip^{k-1}} \equiv \binom{p^{k-j}-rp^{k-j-1}}{ip^{k-j-1}} \pmod{p^{k-j}}, \quad 1\leqslant j\leqslant k-1,$$

в частности,

$$\binom{p^k-rp^{k-1}}{ip^{k-1}} \equiv \binom{p-r}{i} \pmod{p}.$$

Доказательство проводится аналогично.

Следствие 3. При всех $2\leqslant k\leqslant n$r и $1\leqslant i\leqslant p-1$ выполняется сравнение

$$(-1)^i\binom{p^k-p^{k-1}}{ip^{k-1}} \equiv (-1)^i\binom{p-1}{i} \equiv 1 \pmod{p}.$$

Доказательство. С учётом предыдущего следствия достаточно показать, что

$$(-1)^i\binom{p-1}{i} \equiv 1 \pmod p.$$

Воспользуемся индукцией по i. При $i = 1$ сравнение очевидно. Если доказано, что

$$(-1)^{i-1}\binom{p-1}{i-1} \equiv 1 \pmod p,$$

то с учётом $(i, p) = 1$ получаем

$$(-1)^i\binom{p-1}{i} - 1 = (-1)^i\binom{p-1}{i-1} \cdot \frac{p-i}{i} - 1 \equiv (-1)\left(\frac{p-i}{i} + 1\right) \equiv 0 \pmod p.$$

Следствие доказано. ■

2. Сведение к случаю примарных циклических групп

Покажем, что параметр dl F в случае, когда на множестве аргументов и значений заданы структуры циклических групп, может принимать конечные значения только тогда, 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, причём dl $F < \infty$, то выполнены равенства $g = p^n$ и $h = p^k$ при некоторых простом $p \geqslant 2$, натуральных $n \geqslant 1$ и $k \geqslant 1$.

Доказательство. Рассмотрим сначала случай $m = 1$. Пусть p — простой делитель числа h и $F'(x) = F(x) \pmod p$, $x \in G$. Представим значения функции F в виде вектора $(F'(1), \ldots, F'(g-1), F'(0))$. Действие производной Δ_1 на функцию F' можно представить как умножение вектора значений на матрицу A над полем $\mathbb{Z}_p$, где

$$A = \begin{pmatrix} -1 & 0 & \ldots & 0 & 1 \\ 1 & -1 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \ldots & & \ldots & & \ldots \\ 0 & 0 & \ldots & -1 & 0 \\ 0 & 0 & \ldots & 1 & -1 \end{pmatrix}.$$

В этой матрице сумма строк равна нулю. Характеристический многочлен матрицы A над полем $\mathbb{Z}_p$ равен

$$\chi_A(\lambda) = |A - \lambda E| = \lambda\left((-1)^{g-1}(\lambda+1)^{g-1} + (-1)^{g-2}\right) = (-1)^{g-1}\lambda((\lambda+1)^{g-1} - 1) =$$
$$= (-1)^{g-1}\lambda\left(\lambda^{g-1} + \binom{g}{1}\lambda^{g-2} + \binom{g}{2}\lambda^{g-3} + \cdots + \binom{g}{g-2}\lambda + \binom{g}{g-1}\right).$$

При $g = p^n$ все биномиальные коэффициенты в записи характеристического многочлена равны нулю по модулю p (лемма 1). Поэтому $\chi_A(\lambda) = (-1)^{g-1}\lambda^g \pmod p$ и граф линейного преобразования с матрицей A содержит один единичный цикл в точке $(0, 0, \ldots, 0)$, а все остальные векторы лежат на подходах к этому циклу (см., например, [2]). Отсюда следует, что последовательность производных $\Delta_1^i F'$, $i = 1, 2, \ldots$, всегда сходится к нулю.

Если же g не является примарным числом вида p^n, то среди биномиальных коэффициентов в записи характеристического многочлена найдутся не сравнимые с нулем по

модулю p. Поэтому характеристический многочлен $\chi_A(\lambda)$ не равен $(-1)^{g-1}\lambda^g \pmod p$ и в графе линейного преобразования с матрицей A есть циклы, отличные от единичного в точке $(0,0,\dots,0)$. Следовательно, последовательность значений производных при соответствующих значениях аргумента является периодической и степени производной $\Delta_1^i F$ никогда не обратятся в нуль.

Теперь легко видеть, что число h также должно быть примарным. Если оно составное, то, проводя аналогичные рассуждения для делителей числа h, отличных от p, убеждаемся, что сходимость к нулю не будет иметь места.

Пусть теперь $m > 1$. Если для функции от m переменных последовательность производных сходится к нулю, то и для функций от одной переменной, полученных фиксацией всех переменных, кроме одной, также выполнено это свойство. Поэтому, в силу доказанного выше, порядок группы G должен быть примарным числом. ■

Заметим, что теорему 1 можно сформулировать в более общем виде.

Теорема 1′. Если $F : G_1 \times \cdots \times G_m \to H_1 \times \cdots \times H_t$, где G_i и H_j — циклические группы, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant t$, причём $\operatorname{dl} F < \infty$, то найдётся простое число $p \geqslant 2$, такое, что $|G_i| = p^{n_i}$ и $|H_j| = p^{k_j}$ при некоторых $n_i \geqslant 1$, $1 \leqslant i \leqslant m$, $k_j \geqslant 1$, $1 \leqslant j \leqslant t$.

Доказательство по сути остается неизменным.

3. Оценка параметра $\operatorname{dl}(F)$ для функций на примарных циклических группах

Пусть на множестве аргументов и значений произвольной функции $F : G \to H$ задана структура циклической абелевой p-группы примарного порядка: $G = \mathbb{Z}_{p^n}$ и $H = \mathbb{Z}_{p^k}$, $p \geqslant 2$, $n, k \geqslant 1$. Покажем, что параметр $\operatorname{dl} F$ принимает конечное значение.

Теорема 2. Если $F : G \to H$, $G = \mathbb{Z}_{p^n}$, $H = \mathbb{Z}_{p^k}$, $p \geqslant 2$, то

$$\operatorname{dl} F \leqslant p^n + (k-1)(p-1)p^{n-1} - 1.$$

Доказательство. Так как производная суммы функций равна сумме производных, то достаточно рассмотреть случай, когда функция F принимает единственное ненулевое значение. Пусть $F(1) = \cdots = F(p^n - 1) = 0$ и $F(0) = 1$. Рассмотрим последовательность производных

$$\Delta_a F, \quad \Delta_a^2 F = \Delta_a \Delta_a F, \quad \Delta_a^3 F = \Delta_a \Delta_a \Delta_a F, \quad \dots$$

Сначала рассмотрим случай $a = 1$. Соберём значения производных в табл. 1 для $p = 2$ и табл. 2 для $p > 2$ (все значения в таблицах приводятся по модулю p^k).

Имеем при $0 \leqslant i \leqslant p^n - 1$

$$\Delta_1^j F(p^n - i) = (-1)^{i+j} \binom{j}{i} \mod p^k.$$

При $i = p^n$ значение $\Delta_1^{p^n} F(0)$ равно 2 при $p = 2$ и нулю при $p > 2$.

Из таблиц и из леммы 1 следует, что производная $\Delta_1^{p^n} F$ является первой, для которой все значения принадлежат идеалу $p\mathbb{Z}_{p^k}$. Сформулируем свойства элементов в строке с номером p^n более точно:

1) p значений, соответствующих значениям аргумента вида ip^{n-1}, $0 \leqslant i < p$, лежат в $p\mathbb{Z}_{p^k}$;
2) $p^2 - p$ значений, соответствующих оставшимся значениям аргумента вида ip^{n-2}, $0 \leqslant i < p^2$, лежат в $p^2\mathbb{Z}_{p^k}$;

Таблица 1

Значения производных $\Delta_1^i F$ для случая $p = 2$

x	1	2	...	2^n-4	2^n-3	2^n-2	2^n-1	0
F	0	0	...	0	0	0	0	1
$\Delta_1 F$	0	0	...	0	0	0	1	-1
$\Delta_1^2 F$	0	0	...	0	0	1	-2	1
$\Delta_1^3 F$	0	0	...	0	1	-3	3	-1
$\Delta_1^4 F$	0	0	...	1	-4	6	-4	1
...	...	...	...	...	...	...	...	...
$\Delta_1^{2^n-1} F$	1	$-(2^n-1)$	...	$-\binom{2^n-1}{4}$	$\binom{2^n-1}{3}$	$-\binom{2^n-1}{2}$	2^n-1	-1
$\Delta_1^{2^n} F$	0	0	...	$\binom{2^n}{4}$	$\binom{2^n}{3}$	$\binom{2^n}{2}$	0	2
...	...	...	...	...	...	...	...	...

Таблица 2

Значения производных $\Delta_1^i F$ для случая $p > 2$

x	1	2	...	p^n-4	p^n-3	p^n-2	p^n-1	0
F	0	0	...	0	0	0	0	1
$\Delta_1 F$	0	0	...	0	0	0	1	-1
$\Delta_1^2 F$	0	0	...	0	0	1	-2	1
$\Delta_1^3 F$	0	0	...	0	1	-3	3	-1
$\Delta_1^4 F$	0	0	...	1	-4	6	-4	1
...	...	...	...	...	...	...	...	...
$\Delta_1^{p^n-1} F$	1	$-(p^n-1)$	...	$\binom{p^n-1}{4}$	$-\binom{p^n-1}{3}$	$\binom{p^n-1}{2}$	$-(p^n-1)$	1
$\Delta_1^{p^n} F$	0	0	...	$-\binom{p^n}{4}$	$\binom{p^n}{3}$	$-\binom{p^n}{2}$	0	0
...	...	...	...	...	...	...	...	...

3) p^3-p^2 значений, соответствующих оставшимся значениям аргумента вида ip^{n-3}, $0 \leqslant i < p^3$, лежат в $p^3\mathbb{Z}_{p^k}$, и т. д.;
4) $p^{n-1} - p^{n-2}$ значений, соответствующих оставшимся значениям аргумента вида ip, $0 \leqslant i < p^{n-1}$, лежат в $p^{n-1}\mathbb{Z}_{p^k}$;
5) остальные $(p-1)p^{n-1}$ элементов лежат в $p^n\mathbb{Z}_{p^k}$.

Из лемм 1–3 следует также, что для других строк выполнены следующие свойства:

1) через каждые p шагов в строках с номерами, кратными p, стоят производные, у которых все значения кратны p, за исключением тех, которые соответствуют аргументам вида ip, $0 \leqslant i < p^{n-1}$;
2) через каждые p^2 шагов в строках с номерами, кратными p^2, стоят производные, у которых все значения кратны p^2, за исключением p^{n-2} значений, соответствующих аргументам вида ip^2, $0 \leqslant i < p^{n-2}$, лежащих в $\mathbb{Z}_{p^k}$, и $p^{n-1}-p^{n-2}$ значений, соответствующих оставшимся значениям аргумента вида ip, $0 \leqslant i < p^{n-1}$, лежащих в $p\mathbb{Z}_{p^k}$, и т. д.;
3) через каждые p^{n-1} шагов в строках с номерами, кратными p^{n-1}, стоят производные, у которых все значения кратны p^{n-1}, за исключением тех, которые соответствуют аргументам вида ip, $0 \leqslant i < p^{n-1}$.

Покажем, что все значения $\Delta_1^{p^n+(p-1)p^{n-1}} F$ лежат в $p^2\mathbb{Z}_{p^k}$.

Для этого представим функцию $\Delta_1^{p^n} F$ в виде суммы $\Delta_1^{p^n} F = F_0 + F_1$, где функция F_0 отличается от $\Delta_1^{p^n} F$ тем, что у неё значения в точках $x = ip^{n-1}$, $i = 1, \ldots, p-1$, те же, а остальные равны нулю. В этом случае все значения функции F_1 лежат в $p^2\mathbb{Z}_{p^k}$.

Рассмотрим значения функции F_0.

С помощью леммы 2 и следствия из неё можно сводить изучение значений элементов по модулю p^{t-1}, стоящих в строке с номером p^t, $1 \leqslant t \leqslant n$, на местах с номерами p^{t-1}, $2p^{t-1}$, …, $(p-1)p^{t-1}$, p^t, к рассмотрению элементов, стоящих в строке с номером p^{t-1} на местах с номерами p^{t-2}, $2p^{t-2}$, …, $(p-1)p^{t-2}$, p^{t-1}, и т. д.

Тем самым фактически для изучения значений элементов таблиц по модулю p, стоящих в строках с номерами ip^{t-1}, $1 \leqslant t \leqslant n$, $0 \leqslant i \leqslant p-1$, можно редуцировать табл. 2, уменьшив её в p^{n-1} раз до размера $p \times p$, и изучить поведение ненулевых по модулю p значений в строках с номерами i, $0 \leqslant i \leqslant p-1$. Пример, иллюстрирующий вид табл. 2 для случая $p = 5$ и $n = k = 2$, приведён в табл. 3.

Таблица 3

Значения производных для случая $p = 5$ и $n = k = 2$

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	0
F	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**
1																								**1**	**24**
2																							**1**	**23**	**1**
3																						**1**	**22**	**3**	**24**
4																					**1**	**21**	**6**	**21**	**1**
5																				**1**	**20**	**10**	**15**	**5**	**24**
6																			1	19	15	5	15	19	1
7																		1	18	21	15	10	4	7	24
8																	1	17	3	19	20	19	3	17	1
9																1	16	11	16	1	24	9	14	9	24
10															**1**	15	20	5	10	**23**	10	5	20	15	**1**
11														1	14	5	10	5	13	12	20	15	20	11	24
12													1	13	16	5	20	8	24	8	20	5	16	13	1
12												1	12	3	14	15	13	16	9	12	10	11	22	13	24
14											1	11	16	11	1	23	3	18	3	23	1	11	16	11	1
15										**1**	10	5	20	15	**22**	5	15	10	20	**3**	10	5	20	15	**24**
16									1	9	20	15	20	7	8	10	20	10	8	7	20	15	20	9	1
17								1	8	11	20	5	12	1	2	10	15	23	24	13	20	5	14	17	24
18							1	7	3	9	10	7	14	1	8	5	8	1	14	7	10	9	3	7	1
19						1	6	21	6	1	22	7	12	7	22	3	18	13	18	3	24	19	4	19	24
20					**1**	5	15	10	20	**21**	10	5	20	15	**6**	15	20	5	10	**21**	20	10	15	5	**1**
21				1	4	10	20	10	1	14	20	15	20	16	9	5	10	5	11	24	15	5	15	21	24
22			1	3	6	10	15	16	13	6	20	5	21	18	21	5	20	6	13	16	15	10	6	3	1
23		1	2	3	4	5	1	22	18	14	10	16	22	3	9	15	11	7	3	24	20	21	22	23	24
24	1	1	1	1	1	21	21	21	21	21	6	6	6	6	6	21	21	21	21	21	21	1	1	1	1
25	0	0	0	0	**20**	0	0	0	0	**10**	0	0	0	0	**15**	0	0	0	0	**5**	0	0	0	0	**0**
26	0	0	0	20	5	0	0	0	10	15	0	0	0	15	10	0	0	0	5	20	0	0	0	0	0
27	0	0	20	10	20	0	0	10	5	10	0	0	15	20	15	0	0	5	15	5	0	0	0	0	0
28	0	20	15	10	5	0	10	20	5	15	0	15	5	20	10	0	5	10	20	20	0	0	0	0	0
29	20	20	20	20	20	10	10	10	10	10	15	15	15	15	15	5	5	5	5	5	0	0	0	0	0
30	0	0	0	0	**15**	0	0	0	0	**5**	0	0	0	0	**15**	0	0	0	0	**20**	0	0	0	0	**20**
31	0	0	0	15	10	0	0	0	5	20	0	0	0	15	10	0	0	0	20	5	0	0	0	20	5
32	0	0	15	20	15	0	0	5	15	5	0	0	0	0	15	0	0	20	10	20	0	0	20	10	20
33	0	15	5	20	10	0	5	10	15	20	0	0	0	0	15	0	20	15	10	5	0	20	15	10	5
34	15	15	15	15	15	5	5	5	5	5	15	15	15	15	15	20	20	20	20	20	20	20	20	20	20
35	0	0	0	0	**15**	0	0	0	0	**10**	0	0	0	0	**5**	0	0	0	0	**0**	0	0	0	0	**20**
36	0	0	0	15	10	0	0	0	10	15	0	0	0	5	20	0	0	0	0	0	0	0	0	20	5
37	0	0	15	20	15	0	0	10	5	10	0	0	5	15	5	0	0	0	0	0	0	0	20	10	20
38	0	15	5	0	10	0	10	20	5	15	0	5	10	15	20	0	0	0	0	0	0	20	15	10	5
39	15	15	15	15	15	10	10	10	10	10	5	5	5	5	5	0	0	0	0	0	20	20	20	20	20
40	0	0	0	0	**20**	0	0	0	0	**20**	0	0	0	0	**20**	0	0	0	0	**20**	0	0	0	0	**20**
41	0	0	0	20	5	0	0	0	20	5	0	0	0	20	5	0	0	0	20	5	0	0	0	20	5
42	0	0	20	10	20	0	0	20	10	20	0	0	20	10	15	0	0	20	10	20	0	0	20	10	20
43	0	20	15	10	5	0	20	15	10	5	0	20	15	10	5	0	20	15	10	5	0	20	15	10	5
44	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20
45	0	0	0	0	**0**	0	0	0	0	**0**	0	0	0	0	**0**	0	0	0	0	**0**	0	0	0	0	**0**

Рассмотрим кратные производные для функции, полученной в результате такого редуцирования. Пусть

$$pR(i) = F_0(ip^{n-1}) = \Delta_1^{p^n} F(ip^{n-1}) \mod p^2, \quad 1 \leqslant i \leqslant p-1,$$

где $R : \mathbb{Z}_p \to \mathbb{Z}_p$ — функция, полученная в результате редуцирования.

Воспользуемся также следующей очевидной леммой.

Лемма 4. Для любой функции $F : G \to G$, $G = \mathbb{Z}_M$, $M > 2$, удовлетворяющей условию

$$\sum_{x=0}^{M-1} F(x) \equiv 0 \pmod M,$$

существует функция $F^* : G \to H$, такая, что $\Delta_1 F^* = F$.

Доказательство. Используя равенства $F(x) = F^*(x+1) - F^*(x)$, $0 \leqslant x \leqslant M-1$, составим систему уравнений в $\mathbb{Z}_M$ для значений функции F^*:

$$\begin{aligned}
F^*(1) &= F^*(0) + F(0),\\
F^*(2) &= F^*(1) + F(1),\\
&\dots \quad \dots\\
F^*(M-1) &= F^*(M-2) + F(M-2),\\
F^*(0) &= F^*(M-1) + F(M-1) = F^*(0) + \sum_{x=0}^{M-1} F(x).
\end{aligned}$$

Теперь, выбирая произвольное значение $F^*(0)$, можно однозначно вычислить все остальные значения функции F^*. ■

В силу леммы 4 можно считать, что сама функция R является производной некоторой функции R^*. Так как для любой функции от одной переменной по модулю p её производная степени p равна нулю, то

$$\Delta_1^{p-1} R = \Delta_1^p R^* = 0 \mod p.$$

Это означает, что $\Delta_1^{p^n+(p-1)p^{n-1}} F(x) = 0 \mod p^2$ при всех $x \in \mathbb{Z}_{p^n}$. (Другой способ доказательства этого факта основан на следствии 3. Если увеличить на 1 значения функции F_0 в точках ip^{n-1}, то получаются значения, кратные p, причем значения последующих производных в этих точках не изменятся. Поэтому через p^n шагов все значения будут кратны p^2.)

Для рассмотренного выше примера из табл. 3 для $p^n = 25$ функция R и её производные приведены в табл. 4.

Таблица 4

Значения производных функции R для случая $p = 5$ и $n = k = 2$

x	1	2	3	4	0
R^*	0	4	1	4	0
R	4	2	3	1	0
$\Delta_1^1 R$	3	1	3	4	4
$\Delta_1^2 R$	3	2	1	0	4
$\Delta_1^3 R$	4	4	4	4	4
$\Delta_1^4 R$	0	0	0	0	0

Теперь строка значений функции $\Delta_1^{p^n+(p-1)p^{n-1}} F$ обладает свойствами, аналогичными рассмотренной выше строке значений $\Delta_1^{p^n} F$:

1) p значений, соответствующих значениям аргумента вида ip^{n-1}, $0 \leqslant i < p$, лежат в $p^2\mathbb{Z}_{p^k}$;
2) $p^2 - p$ значений, соответствующих оставшимся значениям аргумента вида ip^{n-2}, $0 \leqslant i < p^2$, лежат в $p^3\mathbb{Z}_{p^k}$;
3) $p^3 - p^2$ значений, соответствующих оставшимся значениям аргумента вида ip^{n-3}, $0 \leqslant i < p^3$, лежат в $p^4\mathbb{Z}_{p^k}$, и т. д.;
4) $p^{n-2} - p^{n-3}$ значений, соответствующих оставшимся значениям аргумента вида ip^2, $0 \leqslant i < p^{n-2}$, лежат в $p^{n-1}\mathbb{Z}_{p^k}$;
5) остальные $p^n - p^{n-2}$ элементов лежат в $p^n\mathbb{Z}_{p^k}$.

Аналогично рассуждая, получаем, что все значения $\Delta_1^{p^n+2(p-1)p^{n-1}}F$ лежат в $p^3\mathbb{Z}_{p^k}$, и т. д. Таким образом, при

$$N = p^n + (k-1)(p-1)p^{n-1}$$

для всех $x \in \mathbb{Z}_{p^n}$ выполнено равенство

$$\Delta_1^N F(x) = 0 \mod p^k.$$

Теперь рассмотрим случай произвольной последовательности кратных производных. При $1 < a \leqslant p^n - 1$ равенство $\Delta_a^N F = 0 \mod p^k$ также остается справедливым. Это вытекает из следующей леммы.

Лемма 5. Для любой функции $F : \mathbb{Z}_M \to \mathbb{Z}_M$ и любого $1 < a < M$ справедливо равенство

$$\Delta_a F(x) = \Delta_1 \left(\sum_{i=0}^{a-1} F(x+i) \right).$$

Доказательство вытекает из очевидного равенства

$$F(x+a) - F(x) = \sum_{i=0}^{a-1} (F(x+i+1) - F(x+i)).$$

Рассмотрим кратную производную $\Delta_{a_1}\Delta_{a_2}\dots\Delta_{a_N}F$ для произвольной последовательности $a_1, a_2 \dots, a_N \in \mathbb{Z}_{p^n}$. Очевидным следствием леммы 5 является

Лемма 6. Для любой функции $F : \mathbb{Z}_M \to \mathbb{Z}_M$ и любых $1 < a_i < M$, $1 \leqslant i \leqslant N$, справедливо равенство

$$\Delta_{a_1}\Delta_{a_2}\dots\Delta_{a_N}F(x) = \sum_{i_1=0}^{a_1-1} \dots \sum_{i_N=0}^{a_N-1} \Delta_1^N F(x + i_1 + \dots + i_N).$$

Из леммы 6 вытекает, что при $N = p^n + (k-1)(p-1)p^{n-1}$ все кратные производные степени N обращаются в нуль. Следовательно, $\mathrm{dl}\, F \leqslant p^n + (k-1)(p-1)p^{n-1} - 1$. ■

Перейдём теперь к случаю нескольких переменных.

Теорема 3. Если $F : G_1 \times \dots \times G_m \to H$, $G_i = \mathbb{Z}_{p^{n_i}}$, $1 \leqslant i \leqslant m$, $H = \mathbb{Z}_{p^k}$, $p \geqslant 2$, то

$$\mathrm{dl}\, F \leqslant \sum_{i=1}^{m} (p^{n_i} - (k-1)(p-1)p^{n_i-1} - 1).$$

Доказательство. Рассмотрим случай $m = 2$. При всех $a_1, a_2 \in \mathbb{Z}_{p^n}$ имеем

$$\Delta_{(a_1,a_2)}F(x_1,x_2) = \Delta_{(a_1,0)}F(x_1,x_2+a_2) + \Delta_{(0,a_2)}F(x_1,x_2).$$

Пользуясь леммой 5, получаем при всех $a_1, a_2, b_1, b_2 \in \mathbb{Z}_{p^n}$

$$\Delta_{(b_1,b_2)}\Delta_{(a_1,a_2)}F(x_1,x_2) = \Delta_{(b_1,b_2)}\left(\Delta_{(1,0)}\sum_{i=0}^{a_1-1}F(x_1+i,x_2+a_2)+\Delta_{(0,1)}\sum_{j=0}^{a_2-1}F(x_1,x_2+j)\right) =$$
$$= \Delta^2_{(1,0)}H_{1,0}(x_1,x_2)+\Delta_{(1,0)}\Delta_{(0,1)}H_{1,1}(x_1,x_2)+\Delta^2_{(0,1)}H_{0,1}(x_1,x_2)$$

при некоторых функциях $H_{1,0}, H_{1,1}$ и $H_{0,1}$.

Следовательно, каждую кратную производную степени N

$$\Delta_{(a_1^{(1)},\,a_2^{(1)})}\dots\Delta_{(a_1^{(N)},\,a_2^{(N)})}F(x_1,x_2)$$

можно преобразовать к виду

$$\sum_{i=0}^{N}\Delta^i_{(1,0)}\Delta^{N-i}_{(0,1)}F_{i,N-i}(x_1,x_2)$$

при некоторых функциях $F_{i,N-i}$, $0 \leqslant i \leqslant N$.

Для того чтобы все кратные производные обратились в нуль, достаточно, чтобы число i было больше, чем $p^{n_1}+(k-1)(p-1)p^{n_1-1}$, или число $(N-i)$ — больше, чем $p^{n_2}+(k-1)(p-1)p^{n_2-1}$. Значит, при

$$N = (p^{n_1}+(k-1)(p-1)p^{n_1-1}-1)+(p^{n_2}+(k-1)(p-1)p^{n_2-1}-1)+1$$

все производные будут равны нулю. Отсюда в случае $m=2$ справедлива оценка

$$\mathrm{dl}\,F \leqslant (p^{n_1}+(k-1)(p-1)p^{n_1-1}-1)+(p^{n_2}+(k-1)(p-1)p^{n_2-1}-1).$$

В общем случае имеем оценку $\mathrm{dl}\,F \leqslant \sum\limits_{i=1}^{m}(p^{n_i}+(k-1)(p-1)p^{n_i-1}-1)$. ■

Теорема 4. Пусть $F : G_1\times\dots\times G_m \to H_1\times\dots\times H_t$, где $G=\mathbb{Z}_{p^{n_i}}$, $H=\mathbb{Z}_{p^{k_j}}$, $1\leqslant i\leqslant m$, $1\leqslant j\leqslant t$; $p\geqslant 2$; $m\geqslant 1$; $t\geqslant 1$. Если $F=(F_1,\dots,F_t)$, где F_j — соответствующие координатные функции $F_j : G_1\times\dots\times G_m \to H_j$, $1\leqslant j\leqslant t$, то

$$\mathrm{dl}\,F = \max_{1\leqslant j\leqslant t}\mathrm{dl}\,F_i \leqslant \sum_{i=1}^{m}\left(p^{n_i}+\left(\max_{1\leqslant j\leqslant t}k_j-1\right)(p-1)p^{n_i-1}-1\right).$$

Доказательство вытекает из определения параметра dl и теоремы 3.

Следствие 4. Если $F : G^m \to G^t$, где $G=\mathbb{Z}_{p^n}$, $p\geqslant 2$, $m\geqslant 1$, $t\geqslant 1$, то

$$\mathrm{dl}\,F \leqslant m(p^n+(n-1)(p-1)p^{n-1}-1) = m(p^n n-p^{n-1}(n-1)-1) = m\left(p^n\left(n-\frac{n-1}{p}\right)-1\right).$$

Преимущество данного подхода к определению степени нелинейности заключается в том, что он полностью определяется свойствами только операции сложения. Так, например, из определения степени нелинейности легко вытекает

Теорема 5. 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 $\mathrm{dl}\,(F|_R)\leqslant \mathrm{dl}\,F$.

4. Полиномиальные функции

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 $G = \mathbb{Z}_{p^n}$ и $H = \mathbb{Z}_{p^k}$ 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 (см., например, [3, 4]). Покажем, что для полиномиальных функций над кольцом $\mathbb{Z}_{p^n}$ степень нелинейности функции совпадает с минимальной степенью многочлена, задающего эту функцию.

Теорема 6. Если $F : G^m \to G$ — полиномиальная функция над кольцом $G = \mathbb{Z}_{p^n}$, $p \geqslant 2$, $n \geqslant 1$, $m \geqslant 1$, 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 $P(x_1, \dots x_n)$:

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

Доказательство. Как известно [3], многочлен минимальной степени, задающий функцию F, определён однозначно и может быть записан в виде

$$P(x_1, \dots x_n) = \sum_{1 \leqslant i_1 < \dots < i_l \leqslant n} \; \sum_{i + \alpha(j_1) + \dots + \alpha(j_l) < m} b^{j_1 \dots j_l}_{i_1 \dots i_l i}\, p^i (x_{i_1})_{j_1} \dots (x_{i_l})_{j_l},$$

где $(x)_j = x(x-1)\dots(x-i+1)$, $\alpha(j) = \max\{t : j! \equiv 0 \pmod{p^t}\}$, причём все коэффициенты $b^{j_1 \dots j_l}_{i_1 \dots i_l i}$ являются целыми числами, удовлетворяющими условию $1 \leqslant b^{j_1 \dots j_l}_{i_1 \dots i_l i} \leqslant p-1$.

Из свойств факториальной степени следует, что при всех $1 \leqslant i_1 < \dots < i_l \leqslant n$ и $i + \alpha(j_1) + \dots + \alpha(j_l) < m$

$$\mathrm{dl}\, (x_{i_1})_{j_1} \dots (x_{i_l})_{j_l} = j_1 + \dots + j_l = \deg (x_{i_1})_{j_1} \dots (x_{i_l})_{j_l}.$$

Поэтому

$$\mathrm{dl}\, F \leqslant \max\{j_1 + \dots + j_l\} = \deg P,$$

где максимум берется по всем одночленам, входящим в запись многочлена $P(x_1, \dots x_n)$.

Докажем, что имеет место равенство. Пусть $b^{j_1 \dots j_l}_{i_1 \dots i_l i}\, p^i (x_{i_1})_{j_1} \dots (x_{i_l})_{j_l}$ — один из одночленов максимальной степени. Для него выполняется

$$\Delta^{j_1}_{e_{i_1}} \dots \Delta^{j_l}_{e_{i_l}}\, b^{j_1 \dots j_l}_{i_1 \dots i_l i}\, p^i (x_{i_1})_{j_1} \dots (x_{i_l})_{j_l} = b^{j_1 \dots j_l}_{i_1 \dots i_l i}\, p^i i_1! \dots i_l! \not\equiv 0 \pmod{p^n}.$$

Здесь через e_i обозначен вектор $(0, \dots 0, 1, 0, \dots, 0)$, в котором единица стоит на i-м месте, соответствующем переменной x_i.

Покажем, что все остальные одночлены после взятия производной $\Delta^{j_1}_{e_{i_1}} \dots \Delta^{j_l}_{e_{i_l}}$ обратятся в нуль. Если $b^{q_1 \dots q_s}_{k_1 \dots k_s k}\, p^k (x_{k_1})_{q_1} \dots (x_{k_s})_{q_s}$ — другой одночлен максимальной степени, $j_1 + \dots + j_l = q_1 + \dots + q_s$, для которого

$$\Delta^{j_1}_{e_{i_1}} \dots \Delta^{j_l}_{e_{i_l}}\, b^{j_1 \dots j_s}_{k_1 \dots k_s k}\, p^k (x_{k_1})_{q_1} \dots (x_{k_s})_{q_s} \not\equiv 0 \pmod{p^n},$$

то для наборов переменных должно выполняться включение $\{i_1, \dots, i_l\} \subseteq \{k_1, \dots, k_s\}$, так как иначе взятие производной по несущественной переменной даст нулевое значение. Кроме того, чтобы производная не обращалась в нуль, должны выполняться

неравенства $j_h \leqslant q_h$, $1 \leqslant h \leqslant l$, но это противоречит тому, что одночлены различны. Поэтому

$$\Delta_{e_{i_1}}^{j_1} \dots \Delta_{e_{i_l}}^{j_l} F(x) \equiv b_{i_1 \dots i_l i}^{j_1 \dots j_l} p^i i_1! \dots i_l! \not\equiv 0 \pmod{p^n},$$

откуда окончательно получаем $\mathrm{dl}\, F = j_1 + \dots + j_l = \deg P$. ■

В заключение рассмотрим псевдополиномиальный способ задания функций над кольцом вычетов, в котором вместо факториальных степеней используются биномиальные коэффициенты. Рассмотрим целочисленные функции

$$\binom{x}{i} = \frac{x(x-1)\cdots(x-i+1)}{i!}$$

при $i \in \{1, \dots, n-1\}$, $x \in \mathbb{Z}$. При $i = 0$ полагают $\binom{x}{0} = 1$. При $0 \leqslant a \leqslant b \leqslant n-1$ имеют место соотношения

$$\sum_{i=a}^{b} (-1)^{i+a} \binom{i}{a} \binom{b}{i} = \delta_{ab},$$

где δ_{ab} — символ Кронекера. Если рассматривать функцию $F : \mathbb{Z}_n \to \mathbb{Z}_n$ как целочисленную $F : \mathbb{Z} \to \mathbb{Z}$, принимающую конечное число ненулевых значений в точках $0, 1, \dots, n-1$, то из данных соотношений вытекает справедливость разложения функции $F : \mathbb{Z}_n \to \mathbb{Z}_n$

$$F(x) = \sum_{i=0}^{n-1} h(i) \binom{x}{i}$$

с коэффициентами вида

$$h(i) = \sum_{a=i}^{n-1} F(a)(-1)^{i+a} \binom{i}{a},$$

называемого разложением Ньютона функции F (см., например, [5]).

Для конечной разности $\Delta_1 F(x) = F(x+1) - F(x)$ над $\mathbb{Z}$ справедливы равенства

$$\Delta_1^j \binom{x}{i} = \binom{x}{i-j}, \quad 0 \leqslant j \leqslant i.$$

Поэтому набор коэффициентов $h(i)$, $0 \leqslant i \leqslant n-1$, также можно рассматривать как целочисленную функцию, причём значение $h(i)$ совпадает со значением i-й конечной производной над $\mathbb{Z}$ функции F в точке $x = 0$:

$$h(i) = \Delta_1^i F(0).$$

Для случая нескольких переменных разложение Ньютона строится аналогично:

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

где

$$h(i_1, \dots, i_m) = \Delta_{e_1}^{i_1} \cdots \Delta_{e_m}^{i_m} f(0, \dots, 0), \qquad i_1, \dots, i_m \in \{0, \dots, n-1\},$$

$e_i = (0, \dots, 0, 1, 0, \dots, 0)$ — вектор, i-я координата которого равна 1, $1 \leqslant i \leqslant m$.

Здесь наблюдается кажущееся противоречие с рассмотренным выше подходом, так как максимальная степень нелинейности функции в целочисленном представлении равна $n-1$ (для случая одной переменной), в то время как степень нелинейности

этой же функции над кольцом вычетов может оказаться значительно превосходящей число $n-1$. Различие в значениях степени нелинейности объясняется тем, что действия оператора Δ_1 на множестве целочисленных функций и функций над кольцом вычетов отличаются. Например, над $\mathbb{Z}$ имеем

$$\Delta_1\binom{x}{i} = \binom{x+1}{i} - \binom{x}{i} = \binom{x}{i-1},$$

в то время как над $\mathbb{Z}_n$ имеем

$$\Delta_1\binom{x}{i} = \left(\binom{x+1 \mod n}{i} - \binom{x}{i}\right) \mod n, \quad 0 \leqslant i \leqslant n-1,$$

причём при $x = n-1$ получаются разные выражения. Например, при $n = 25$ и $x = 24$ имеем

$$\Delta_1\binom{x}{5}(24) = \binom{25}{5} - \binom{24}{5} = \binom{24}{5} \equiv 5 - 4 \equiv 1 \pmod{25},$$

в то же время, если аргументы приводить по модулю 25, то

$$\Delta_1\binom{x}{5}(24) = \binom{0}{5} - \binom{24}{5} \equiv 0 - 4 \equiv 21 \pmod{25}.$$

Более подробно о разложении Ньютона можно прочитать, например, в [5].

ЛИТЕРАТУРА

1. *Черемушкин А. В.* Аддитивный подход к определению степени нелинейности дискретной функции // Прикладная дискретная математика. 2010. № 2(8). С. 22–33.
2. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра. Учебник в 2-х т. Т. II. М.: Гелиос АРВ, 2003.
3. *Keller G. and Olson F.* Counting polynomial functions (mod p^n) // Duke Math. J. 1968. V. 35. P. 835–838.
4. *Chen Z.* On polynomial functions from $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \mathbb{Z}_{n_r}$ to $\mathbb{Z}_m$ // Discrete Math. 1996. V. 162. P. 67–76.
5. *Davio M., Deschamps J. P., and Thayse A.* Discrete and switching functions. Budapest: Academiai Kiado, 1974.