

АДДИТИВНЫЙ ПОДХОД К ОПРЕДЕЛЕНИЮ СТЕПЕНИ НЕЛИНЕЙНОСТИ ДИСКРЕТНОЙ ФУНКЦИИ¹

А. В. Черемушкин

Институт криптографии, связи и информатики, г. Москва, Россия

E-mail: avc238@mail.ru

В работе предлагается подход к определению степени нелинейности дискретных функций, заданных на абелевых группах, инвариантный по отношению к введению мультипликативных операций. В качестве приложения введенного понятия описан алгоритм нахождения групп инерции в группе сдвигов для функций p^m -значной логики.

Ключевые слова: дискретные функции, степень нелинейности, группа инерции.

1. Конечные производные и степень нелинейности функций на абелевых группах

Рассмотрим функции $F : G \rightarrow H$, у которых на множествах G и H заданы структуры абелевых групп.

Определим производные по направлению $\Delta_a F$, $a \in G$, функции F равенствами

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

где $x \in G$.

Следующие свойства очевидно вытекают из определения.

A1. При всех $a \in G$ выполняется равенство

$$\Delta_a(F_1 + F_2) = \Delta_a F_1 + \Delta_a F_2.$$

Для обозначения нейтрального элемента групп G и H будем использовать символ 0.

A2. Если $\Delta_a F(0) = 0$ для всех $a \in G$, то и $\Delta_a F(x) = 0$ для всех $a, x \in G$.

A3. При всех $a, b \in G$ выполняется равенство

$$\Delta_{a+b} F(x) = \Delta_a F(x + b) - \Delta_b F(x).$$

A4. При всех $a, b \in G$ выполняется равенство

$$\Delta_a \Delta_b F = \Delta_{a+b} F - \Delta_a F - \Delta_b F.$$

Степенью нелинейности функции $F : G \rightarrow H$ (обозначается $dl\ F$) называется минимальное натуральное число m , такое, что

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

при всех $a_1, \dots, a_{m+1}, x \in G$.

¹Работа выполнена при поддержке гранта Президента РФ НШ №4.2008.10.

Заметим, что степень нелинейности определена не для всех функций и абелевых групп. Например, для функции 6-значной логики F , задающей подстановку $(0, 2, 1, 5)(3)(4)$, последовательность

$$\Delta_1 F, \Delta_1 \Delta_1 F, \Delta_1 \Delta_1 \Delta_1 F, \dots$$

является периодической, причем ни одна из функций этой последовательности не равна тождественно нулю.

Ниже будет показано, что если на множестве аргументов и значений функции задана структура элементарной абелевой группы, то степень нелинейности определена всегда.

Для степени нелинейности функции $F : G \rightarrow H$ выполняются следующие очевидные свойства.

V1. Функция F имеет первую степень нелинейности в том и только в том случае, когда она имеет вид $F(x) = \varphi(x) + a$, $\varphi \in \text{Hom}(G, H)$ — гомоморфизм, $a \in G$.

V2. Если $\text{dl } F$ определена, то $\text{dl } F$ — это максимальное m , такое, что при некоторых $a_1, \dots, a_m \in G$

$$\Delta_{a_1} \dots \Delta_{a_m} F(0) \neq 0.$$

Вытекает из свойства A2 производных.

V3. Если $\text{dl } F$ определена, то $\text{dl } \Delta_a F \leq \text{dl } F - 1$ при всех $0 \neq a \in \Omega$, причем всегда найдется такой элемент $0 \neq a \in \Omega$, что $\text{dl } \Delta_a F = \text{dl } F - 1$.

V4. Если $\text{dl } F$ определена, то для любых функций $F_1(x) = \psi(x) + a$, $F_2(x) = \varphi(x) + b$, где $\psi \in \text{End}(G)$, $\varphi \in \text{End}(H)$ — эндоморфизмы, $a \in G$, $b \in H$, выполнено равенство

$$\text{dl } F = \text{dl } (F_2 \circ F \circ F_1),$$

где $\circ$ — операция композиции отображений, $(F_2 \circ F \circ F_1)(x) = F_2(F(F_1(x)))$.

V5. Если для функций $F_i : G \rightarrow H$, $i = 1, 2$, определены $\text{dl } F_1$ и $\text{dl } F_2$, то

$$\text{dl } (F_1 + F_2) \leq \max\{\text{dl } F_1, \text{dl } F_2\}.$$

2. Конечные производные функций на элементарных абелевых группах

Пусть на множестве аргументов и значений произвольной функции $F : G \rightarrow H$ заданы структуры элементарных абелевых p -групп. Если естественным образом рассматривать элементарные абелевы группы как векторные пространства над полем $\text{GF}(p) = \mathbf{Z}_p$, $G = \mathbf{Z}_p^n$ и $H = \mathbf{Z}_p^k$, то функция F задается набором координатных функций $(F_1, \dots, F_k)$. Поэтому помимо введенного выше «аддитивного» определения степени нелинейности, вычисляемого с помощью производных по направлению, можно применять обычное «мультипликативное» определение степени отображения как максимума степеней многочленов координатных функций (см. [1]).

Покажем, что эти два подхода к определению степени нелинейности в данном случае совпадают.

Заметим, что можно рассматривать и более общий случай функций p^m -значной логики $F : \Omega^n \rightarrow \Omega^k$, где на множестве Ω задана структура элементарной абелевой p -группы. Если на множестве Ω ввести дополнительно операцию умножения так, чтобы Ω приобрело структуру конечного поля $\text{GF}(q)$, $q = p^m$, то также можно показать, что «аддитивное» определение степени нелинейности совпадает с «мультипликативным» (см. ниже). Отсюда, в частности, вытекает, что способ введения операции умножения не влияет на значение степени нелинейности функций.

Помимо перечисленных выше свойств А1–А4 производных из-за введения операции умножения оказываются справедливыми также следующие.

А5. При всех $a \in \Omega^n$ выполняется равенство

$$\Delta_a F_1 F_2(x) = \Delta_a F_1(x) F_2(x) + F_1(x+a) \Delta_a F_2(x).$$

Если функции F_1 и F_2 существенно зависят от непересекающихся множеств аргументов: $F_1(x) = f_1(x')$ и $F_2(x) = f_2(x'')$, $x = (x', x'')$, $a = (a', a'')$, то

$$\Delta_a F_1 F_2(x) = \Delta_a f_1 f_2(x) = \Delta_{a'} f_1(x') f_2(x'') + f_1(x') \Delta_{a''} f_2(x'').$$

А6. Для функции $F : \Omega \rightarrow \Omega$ справедливо разложение в точке $x = 0$:

$$F(x) = F(0) - \sum_{j=1}^{q-1} x^j \sum_{0 \neq a \in \text{GF}(q)} \frac{\Delta_a F(0)}{a^j}.$$

Пятое свойство очевидно. Шестое свойство вытекает из формулы

$$h(i) = - \sum_{0 \neq a \in \text{GF}(q)} \frac{f(a)}{a^i}, \quad i \neq 0,$$

для коэффициентов разложения функции

$$f(x) = \sum_{i=0}^{q-1} h(i) x^i.$$

Здесь использовано равенство

$$\sum_{j=1}^{q-1} \left(\frac{x}{a}\right)^j = \begin{cases} -1, & x = a; \\ 0, & x \neq a, \end{cases}$$

справедливое для элементов поля $\text{GF}(q)$.

Особо отметим свойства производных при $a = 1$. Напомним, что факториальные степени определяются равенствами

$$(x)_i = \begin{cases} x(x-1) \dots (x-i+1), & i \geq 0; \\ 1, & i = 0. \end{cases}$$

Факториальные степени связаны с обычными степенями соотношениями:

$$(x)_n = \sum_{j=0}^n s(n, j) x^j; \tag{1}$$

$$x^i = \sum_{j=0}^n \sigma(n, j) (x)_j, \tag{2}$$

где $s(n, j)$ и $\sigma(n, j)$ — коэффициенты, которые для числовых полей называются числами Стирлинга первого и второго рода соответственно. Кроме того, при $0 \leq i \leq n$ справедливы равенства (в поле $\text{GF}(p^n)$):

$$\text{А7. } \Delta_1^i (x)_n = (n)_i (x)_{n-i};$$

$$A8. \Delta_1^i x^n = \sum_{j=0}^n \sigma(n, j)(j)_i (x)_{j-i};$$

$$A9. \Delta_1^n (x)_n = n!.$$

Доказательство этих свойств осуществляется несложной проверкой.

Так как данные равенства рассматриваются как соотношения в поле $GF(p^m)$, то для получения нетривиальных соотношений имеет смысл ограничиться случаем $0 \leq i \leq n \leq p-1$.

В случае, когда a — произвольный элемент поля, не обязательно равный единице, можно положить

$$(x)_{i,a} = \begin{cases} x(x-a)(x-2a)\dots(x-(i-1)a), & i \geq 0; \\ 1, & i = 0. \end{cases}$$

Тогда после замены x на ax получаем аналогичные равенства:

$$(x)_{n,a} = \sum_{j=0}^n s(n, j)a^{n-j}x^j; \quad (3)$$

$$x^i = \sum_{j=0}^n \sigma(n, j)a^{n-j}(x)_{j,a}. \quad (4)$$

Теперь последние три свойства можно сформулировать в более общем виде:

$$A7'. \Delta_a^i (x)_{n,a} = (n)_i a^i (x)_{n-i,a};$$

$$A8'. \Delta_a^i x^n = \sum_{j=0}^n \sigma(n, j)a^{n-j+i}(j)_i (x)_{j-i,a};$$

$$A9'. \Delta_a^n (x)_{n,a} = n!a^n.$$

3. Степень нелинейности функции p^m -значной логики

Пусть, как и выше, на множестве Ω задана структура конечного поля $GF(p^m)$. Согласно введенному выше определению, степенью нелинейности $dl F$ функции p^m -значной логики F называется минимальное натуральное число m , такое, что

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

при всех $a_1, \dots, a_{m+1} \in \Omega$.

Из свойства A5 производных вытекает следующее очевидное свойство степени нелинейности произведения функций.

B6. $dl(F_1 \cdot F_2) \leq dl F_1 + dl F_2$. Если функции F_1 и F_2 зависят от непересекающихся множеств переменных, то $dl(F_1 \cdot F_2) = dl F_1 + dl F_2$.

Стандартное «мультипликативное» значение степени нелинейности p^m -значной функции F , заданной над конечным полем, называемое также индексом нелинейности, определяется как максимальное значение величины

$$\|b_1\| + \dots + \|b_n\|$$

для всех входящих в многочлен функции одночленов $x_1^{b_1} \dots x_n^{b_n}$, $b_i \in \{0, 1, \dots, p^m - 1\}$, $1 \leq i \leq n$, где $\|b_i\|$ — сумма цифр в p -ичной записи числа b_i , $1 \leq i \leq n$.

Как показывают следующие три свойства, эти определения в данном случае равносильны. Сначала установим равносильность для случая $m = 1$.

B7. Для функций над полем $GF(p)$ степень нелинейности и степень функции совпадают.

Доказательство. Пусть $f(x_1, \dots, x_n)$, $n \geq 1$, — произвольная функция, многочлен которой имеет степень $\deg f$, причем все переменные входят в степенях не выше $p-1$. Из свойств В1–В3 степени нелинейности следует, что $\text{dl } f \leq \deg f$. Докажем обратное неравенство.

Воспользуемся индукцией по числу n . Если $n = 1$ и $\deg f = k$, причем

$$f(x) = c_k x^k + c_{k-1} x^{k-1} + \dots + c_1 x + c_0,$$

то, согласно равенству (2) и свойству А9, имеем $\Delta_1^k f(x) = c_k k! \neq 0$.

Предположим, что утверждение справедливо для всех функций от $n-1$ переменного. Пусть $\deg f = k \geq 2$ и в многочлен функции f входит одночлен $x_1^{b_1} \cdot \dots \cdot x_s^{b_s}$, $\sum_{i=1}^s b_i = k$, $s \geq 1$. Разложим многочлен функции f по первой переменной:

$$\begin{aligned} f(x_1, \dots, x_n) &= x_1^k f_k(x_2, \dots, x_n) + x_1^{k-1} f_{k-1}(x_2, \dots, x_n) + \dots \\ &\dots + x_1 f_1(x_2, \dots, x_n) + f_0(x_2, \dots, x_n). \end{aligned}$$

Тогда для вектора $a = (1, 0, \dots, 0) \in \text{GF}(p)^n$ выполнено

$$\Delta_1^{b_1} f(x_1, \dots, x_n) = \Delta_1^{b_1} x_1^{b_1} \cdot f_k(x_2, \dots, x_n) = b_1! \cdot f_k(x_2, \dots, x_n).$$

По предположению индукции функция f_k имеет степень нелинейности $k - b_1$, поэтому найдется набор векторов $a_1, \dots, a_{k-b_1} \in \text{GF}(p)^n$, такой, что

$$\Delta_{a_1} \dots \Delta_{a_{k-b_1}} f(x_2, \dots, x_n) \neq 0.$$

Отсюда следует, что $\text{dl } f \geq k$.

В8. Если при фиксации базиса поля $\text{GF}(p^m)$, рассматриваемого как пространство над $\text{GF}(p)$, функция $F : \text{GF}(p^m)^n \rightarrow \text{GF}(p^m)$, $n \geq 1$, задается в координатном виде набором многочленов $f_1, \dots, f_m$ над полем $\text{GF}(p)$ от mn переменных, то

$$\text{dl } F = \max_{i=\overline{1, n}} \text{dl } f_i.$$

Доказательство. Пусть $e_1, \dots, e_m$ — стандартный базис и функция F задается в координатном виде выражением

$$F(x_1, \dots, x_n) = \sum_{j=1}^m e_j f_j(x_{1,1}, \dots, x_{1,n}, \dots, x_{m,1}, \dots, x_{m,n}),$$

где значения переменных в обеих частях равенства связаны соотношениями $x_i = \sum_{j=1}^m x_{i,j} e_j$, $j = \overline{1, n}$, $i = \overline{1, m}$.

Заметим, что каждая координата $x_{i,j}$, $j = \overline{1, n}$, выражается через x_i , $i = \overline{1, n}$, как линейная функция $\text{tr}(a_{i,j} x_i)$ ($\text{tr}(x) = \sum_{t=0}^{m-1} x^{p^t}$ — функция след) при некотором $a_{i,j} \in \text{GF}(p^m)$. Подставляя эти выражения в правую часть равенства и используя свойства В1–В3 степени нелинейности, получаем оценку

$$\text{dl } F \leq \max_{i=\overline{1, n}} \text{dl } f_i.$$

С другой стороны, если

$$\max_{i=\overline{1, n}} \text{dl } f_i = \text{dl } f_s = k,$$

то по определению найдутся элементы $a_1, \dots, a_k \in \text{GF}(p)^{mn}$, такие, что

$$\Delta_{a_1} \dots \Delta_{a_k} f_s \neq 0.$$

Отсюда, с учетом того, что абелевы группы полей $\text{GF}(p)^{mn}$ и $\text{GF}(p^m)^n$ совпадают, получаем

$$\Delta_{a_1} \dots \Delta_{a_k} f = \sum_{i=1}^m e_i \Delta_{a_1} \dots \Delta_{a_k} f_i \neq 0,$$

то есть

$$\text{dl } F \geq \max_{i=1, n} \text{dl } f_i.$$

B9. Степень нелинейности одночлена

$$x_1^{b_1} \dots x_n^{b_n},$$

где $b_i \in \{0, 1, \dots, p^m - 1\}$, $i = 1, \dots, n$, совпадает с

$$\|b_1\| + \dots + \|b_n\|,$$

где $\|b_i\|$ — сумма цифр в p -ичной записи числа b_i , $1 \leq i \leq n$. Степень нелинейности многочлена над полем $\text{GF}(p^m)$ совпадает с максимальной степенью нелинейности для входящих в него одночленов.

Доказательство. Рассмотрим сначала случай $n = 1$. Так как при $m = 1$ это утверждение по сути уже доказано (см. свойство B7), то рассмотрим случай $m \geq 2$.

Пусть $0 \leq k \leq (p - 1)m$.

Покажем, что множество $\mathcal{U}_k$ многочленов, в которых все входящие в них одночлены x^b , $b \in \{0, 1, \dots, p^m - 1\}$, удовлетворяют неравенству $\|b\| \leq k$, совпадает с множеством $\mathcal{U}'_k$ многочленов, степень нелинейности которых не превосходит k .

Обозначим через $M(p, m, k)$ число разбиений числа k на m неотрицательных слагаемых, каждое из которых не превосходит $p - 1$. Тогда

$$|\mathcal{U}_k| = \sum_{t=0}^k 2^{M(p, m, t)}.$$

С другой стороны, согласно свойству B8, множество $\mathcal{U}'_k$ совпадает с множеством функций, которые задаются в координатном виде набором многочленов $f_1, \dots, f_m$ над полем $\text{GF}(p)$ от m переменных степени нелинейности k . Как нетрудно проверить, множество $\mathcal{U}'_k$ имеет в точности такую же мощность:

$$|\mathcal{U}'_k| = \sum_{t=0}^k 2^{M(p, m, t)}.$$

В силу очевидного неравенства $\text{dl } x^b \leq \|b\|$, которое вытекает из представления

$$x^b = x^{b^{(0)}} \cdot x^{p^1 b^{(1)}} \cdot \dots \cdot x^{p^{m-1} b^{(m-1)}},$$

$b = \sum_{i=0}^{m-1} p^i b^{(i)}$, $\sum_{i=1}^s b^{(i)} = \|b\|$, выполняется включение $\mathcal{U}_k \subseteq \mathcal{U}'_k$. Отсюда получаем $\mathcal{U}_k = \mathcal{U}'_k$.

При $n \geq 2$ рассуждения полностью аналогичны, за исключением того, что в данном случае

$$|\mathcal{U}_k| = |\mathcal{U}'_k| = \sum_{t=0}^k 2^{M(p, mn, t)}.$$

В10. Степень нелинейности функции p^n -значной логики для случая элементарных абелевых групп определяется только свойствами операции сложения. Поэтому для заданной элементарной абелевой p -группы при любом способе задания операции умножения так, чтобы в результате получилось поле из p^n элементов, степень нелинейности функций всегда будет инвариантна по отношению к выбору операции умножения.

В11. Если G , H и R — элементарные абелевы p -группы, $F_1 : G \rightarrow H$, $F_2 : H \rightarrow R$ и $\circ$ — операция композиции отображений $(F_1 \circ F_2)(x) = F_1(F_2(x))$, $x \in G$, то

$$\text{dl}(F_1 \circ F_2) \leq \text{dl } F_1 \cdot \text{dl } F_2.$$

Пусть $|G| = p^n$, $|H| = p^m$ и $|R| = p^k$. В силу свойства В8 достаточно предполагать, что на множествах элементов групп G , H и R заданы структуры $\text{GF}(p)^n$, $\text{GF}(p)^m$ и $\text{GF}(p)^k$. Тогда функции F_1 и F_2 можно задать системами из m и k уравнений от n и m переменных соответственно над полем $\text{GF}(p)$. По свойству В8 степень нелинейности совпадает с максимумом степеней одночленов в многочленах, задающих эти уравнения. Остается подставить во вторую систему вместо аргументов многочлены уравнений первой системы и воспользоваться свойством В5.

В12. Если G и H — элементарные абелевы p -группы и $R \leq G$ — подгруппа в G , то для степеней нелинейности функции $F : G \rightarrow H$ и ее ограничения $F|_R : R \rightarrow H$ на подгруппу R выполнено неравенство $\text{dl}(F|_R) \leq \text{dl } F$.

Это свойство очевидно вытекает из определения степени нелинейности.

В заключение заметим, что вопрос о свойствах аддитивного определения степени нелинейности функций для случая задания на множествах их аргументов и значений других типов групп, например, примарных циклических, остается пока открытым.

4. Вычисление групп инерции функции p^m -значной логики в группе сдвигов

В качестве применения введенного выше понятия степени нелинейности рассмотрим метод нахождения групп инерции функций p^m -значной логики в группе сдвигов, основанный на группировке одночленов в многочленах функций p^m -значной логики по степеням нелинейности.

Пусть $F : \Omega^n \rightarrow \Omega$ — функция p^m -значной логики, причем считаем, что $\Omega = \text{GF}(p^m)$. Группа инерции $(H_n)_F$ этой функции в группе сдвигов H_n относительно операции сложения в поле $\text{GF}(p^m)$ состоит из преобразований $\begin{pmatrix} x \\ x + a \end{pmatrix}$ сдвига на векторы $a = (a_1, \dots, a_n)$, где $a_1, \dots, a_n \in \text{GF}(p^m)$, таких, что

$$F(x_1 + a_1, \dots, x_n + a_n) = F(x_1, \dots, x_n)$$

при всех $x_1, \dots, x_n \in \text{GF}(p^m)$.

Ниже будет описан метод, позволяющий вычислять группу инерции $(H_n)_F$ по известному многочлену функции $F(x_1, \dots, x_n)$ над полем $\text{GF}(p^m)$. Обозначим этот многочлен $f(x_1, \dots, x_n)$.

В основе метода лежит сведение исходной задачи к решению нескольких систем уравнений над полем $\text{GF}(p^m)$, являющихся линейными над полем $\text{GF}(p)$. Поэтому сначала, следуя [2], напомним способ решения таких систем.

4.1. Решение систем p -линейных уравнений

1. Под линейным (над $\text{GF}(p)$) отображением $L : \text{GF}(p^m) \rightarrow \text{GF}(p^m)$ будем понимать произвольный эндоморфизм поля $\text{GF}(p^m)$, рассматриваемого как линейное пространство $(\Omega, +)$ над полем $\text{GF}(p)$. Многочлен $l(x)$, представляющий линейное отображение L над полем $\text{GF}(p)$, называется p -многочленом (см. [2]).

Как известно, произвольный p -многочлен имеет вид

$$l(x) = \sum_{i=0}^{m-1} a_i x^{p^i},$$

где $a_i \in \text{GF}(p^m)$, $i \in \overline{1, m-1}$. Если зафиксировать какой-либо базис $e_1, \dots, e_m$ поля $\text{GF}(p^m)$ над полем $\text{GF}(p)$, то L , как линейное отображение векторного пространства, однозначно задается некоторой матрицей размера $m \times m$ с элементами из поля $\text{GF}(p)$.

Таким образом, решение одного уравнения $L(x) = 0$ над полем $\text{GF}(p^m)$ сводится к решению системы из m линейных уравнений над полем $\text{GF}(p)$. Чтобы выписать эту систему, выразим элементы $L(e_i)$ в базисе $e_1, \dots, e_m$ векторного пространства $(\Omega, +)$:

$$L(e_i) = \sum_{k=1}^{m-1} b_{ik} e_k, \quad i \in \overline{1, m-1}.$$

Тогда при

$$x = \sum_{i=1}^{m-1} x^{(i)} e_i,$$

где $x^{(i)} \in \text{GF}(p)$, $i \in \overline{1, m}$, получаем

$$L(x) = L\left(\sum_{i=1}^{m-1} x^{(i)} e_i\right) = \sum_{i=1}^{m-1} x^{(i)} L(e_i) = (x^{(1)}, \dots, x^{(m)}) B_L$$

при некоторой матрице $B_L = (b_{ij})$. Теперь искомая система уравнений принимает вид

$$(x^{(1)}, \dots, x^{(m)}) B_L = (0, \dots, 0).$$

2. Рассмотрим теперь систему уравнений над полем $\text{GF}(p^m)$ с линейными над $\text{GF}(p)$ многочленами. Ее можно записать в виде

$$\begin{cases} L_{11}(x_1) + \dots + L_{1n}(x_n) = 0, \\ \dots \\ L_{k1}(x_1) + \dots + L_{kn}(x_n) = 0, \end{cases} \quad (5)$$

где L_{ij} — p -многочлены, $i \in \overline{1, k}$, $j \in \overline{1, n}$. Как и выше, зафиксируем некоторый базис поля $\text{GF}(p^m)$, рассматриваемого как линейное пространство над полем $\text{GF}(p)$. Сопоставим каждому многочлену L_{ij} $n \times m$ -матрицу B_{ij} аналогично тому, как это было сделано выше. Тогда система (5) может быть записана в виде системы линейных уравнений над полем $\text{GF}(p)$

$$\left(x_1^{(1)}, \dots, x_1^{(m)}, \dots, x_n^{(1)}, \dots, x_n^{(m)}\right) \begin{pmatrix} B_{11} & \dots & B_{k1} \\ \dots & \dots & \dots \\ B_{1n} & \dots & B_{kn} \end{pmatrix} = (0, \dots, 0). \quad (6)$$

Теперь всякому решению системы (6) соответствует решение

$$(x_1, \dots, x_n) = \left(\sum_{i=1}^m x_1^{(i)} e_i, \dots, \sum_{i=1}^m x_n^{(i)} e_i\right)$$

системы (5).

4.2. Расширения группы инерции

Определим цепочки расширений группы инерции, используя сравнения функций с точностью до многочленов степени нелинейности не выше s , $0 \leq s \leq (p-1)mn$.

Множество функций $F : \text{GF}(p^m)^n \rightarrow \text{GF}(p^m)$, степень нелинейности которых не превосходит s , обозначим через

$$\mathcal{U}_s = \{F(x_1, \dots, x_n) : \text{dl } F \leq s\}.$$

При $s = -1$ полагаем $\mathcal{U}_{-1} = \{0\}$.

Несложно проверить, что множество $\mathcal{U}_s$ является векторным пространством над полем $\text{GF}(p^m)$, в частности, $\mathcal{U}_s$ замкнуто относительно операций сложения функций и умножения на элементы поля $\text{GF}(p^m)$. Введем также множества

$$(\text{H}_n)_F^{(s)} = \left\{ \begin{pmatrix} x \\ x+a \end{pmatrix} \in \text{H}_n : F(x+a) - F(x) \in \mathcal{U}_s \right\}.$$

Несложно проверить, что при любом $s \geq -1$ множество $(\text{H}_n)_F^{(s)}$ является подгруппой группы H_n . В частности, при $s = -1$ выполнено равенство

$$(\text{H}_n)_F^{(-1)} = \left\{ \begin{pmatrix} x \\ x+a \end{pmatrix} \in \text{H}_n : F(x+a) = F(x) \right\} = (\text{H}_n)_F.$$

С другой стороны, по свойству В1 степени нелинейности $\Delta_a F(x) \in \mathcal{U}_{\text{dl } F-1}$, следовательно,

$$(\text{H}_n)_F^{(\text{dl } F-1)} = \text{H}_n.$$

Поэтому первой нетривиальной группой может быть только группа $(\text{H}_n)_F^{(\text{dl } F-2)}$.

Каждой группе $(\text{H}_n)_F^{(s)}$ можно однозначно поставить в соответствие подпространство

$$W_s = \left\{ a = (a_1, \dots, a_n) \in \text{GF}(p^m)^n : \begin{pmatrix} x \\ x+a \end{pmatrix} \in (\text{H}_n)_F^{(s)} \right\}.$$

Очевидны следующие цепочки включений:

$$\begin{aligned} \{0\} &= \mathcal{U}_{-1} \subseteq \mathcal{U}_0 \subseteq \dots \subseteq \mathcal{U}_{(p-1)nm}, \\ (\text{H}_n)_F &= (\text{H}_n)_F^{(-1)} \subseteq \dots \subseteq (\text{H}_n)_F^{(s)} \subseteq \dots \subseteq (\text{H}_n)_F^{(\text{dl } F-1)} = \text{H}_n, \\ W_{-1} &\subseteq W_0 \subseteq \dots \subseteq W_{\text{dl } F-1} = \text{GF}(p^m)^n. \end{aligned}$$

4.3. Метод нахождения групп инерции

Рассмотрим теперь сам метод нахождения группы инерции.

Пусть функция $F(x_1, \dots, x_n) \in \mathcal{U}_k$ представима многочленом $f(x_1, \dots, x_n)$ степени нелинейности $\text{dl } F = k$, $1 \leq k \leq (p-1)nm$.

Рассмотрим многочлен

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

где $x = (x_1, \dots, x_n)$, $a = (a_1, \dots, a_n) \in \text{GF}(p^m)^n$. Сгруппируем одночлены, входящие в $\Delta_a f$, по степеням нелинейности:

$$\Delta_a f = \sum_{i=0}^{k-1} \sum_{b \in I_i} t_b(a) \tilde{X}_b,$$

где через

$$\tilde{X}_b = x_1^{b_1} \cdot \dots \cdot x_n^{b_n}$$

обозначен произвольный одночлен многочлена $\Delta_a f$, $t_b(a)$ — коэффициент при этом одночлене, а I_i обозначает множество

$$I_i = \left\{ b = (b_1, \dots, b_n) \in \{0, 1, \dots, p^m - 1\}^n : \text{dl } \tilde{X}_b = i \right\}.$$

Как было показано выше, группы $(H_n)_F^{(s)}$ могут быть нетривиальными только при $-1 \leq s \leq \text{dl } F - 2$.

Первым шагом предлагаемого метода является нахождение группы $(H_n)_F^{(\text{dl } F - 2)}$ (или, что то же самое, подпространства W_{k-2}). Ее нахождение сводится к решению системы уравнений

$$\{t_b(a) = 0, \quad b \in I_{k-1},$$

в левой части которой стоят p -линейные по переменной a многочлены $t_b(a)$ (см. утверждение 1 ниже). Используя описанный выше метод решения системы линейных уравнений, находим множество решений W_{k-2} и, следовательно, группу $(H_n)_F^{(k-2)}$.

Далее процесс нахождения группы инерции осуществляется индуктивно по мере убывания значения s , $-1 \leq s \leq k - 2$.

Предположим, что уже найдена группа $(H_n)_F^{(s)}$ и соответственно подпространство W_s для $s \leq k - 2$. Теперь для нахождения множества W_{s-1} надо решить систему уравнений (вообще говоря, нелинейных)

$$\{t_b(a) = 0, \quad b \in I_s. \tag{7}$$

Покажем, что на самом деле эта система является линейной на подпространстве W_s .

Утверждение 1. Система уравнений

$$\{t_b(z) = 0, \quad b \in I_s \tag{8}$$

является системой линейных уравнений относительно $z \in W_s$.

Доказательство. Заметим, что для $z \in W_s$ выполняется включение $\Delta_z f \in \mathcal{U}_s$ по определению группы $(H_n)_F^{(s)}$. Поэтому для всех $z_1, z_2 \in W_s$ по свойствам А3 и А4 производных и свойству В1 степени нелинейности выполняется условие

$$\Delta_{z_1+z_2} f - \Delta_{z_1} f - \Delta_{z_2} f = \Delta_{z_1} f \Delta_{z_2} f \in \mathcal{U}_{s-1},$$

откуда получаем

$$t_b(z_1 + z_2) = t_b(z_1) + t_b(z_2)$$

для всех $z_1, z_2 \in W_s$, $b \in I_s$. Отсюда следует, что

$$t_b(c_1 z_1 + c_2 z_2) = c_1 t_b(z_1) + c_2 t_b(z_2)$$

для всех $z_1, z_2 \in W_s$, $c_1, c_2 \in \text{GF}(p)$, $b \in I_s$, что и означает, что данная система является системой линейных уравнений на пространстве W_s . ■

Таким образом, система (7) при наложении ограничения $a \in W_s$ становится линейной, а множество ее решений образует пространство W_{s-1} .

В результате, последовательно находя подпространства

$$W_{k-2}, W_{k-3}, \dots, W_1, W_0, W_{-1},$$

и решая в них системы линейных уравнений, тем самым находим группу

$$(H_n)_F = \left\{ \begin{pmatrix} x \\ x + a \end{pmatrix} : a \in W_{-1} \right\}.$$

Понятно, что сложность данного алгоритма определяется степенью нелинейности функции (она определяет число шагов алгоритма) и сложностью решения систем линейных уравнений над полем $\text{GF}(p)$ от не более чем mn неизвестных. Поэтому в худшем случае трудоемкость можно оценить величиной $O((\text{dl } F) \cdot (nm)^3)$.

Заметим, что трудоемкость линейно зависит от параметра $\text{dl } F$. Для более точной оценки следует воспользоваться одним из быстрых алгоритмов решения систем уравнений, а также учесть, что число неизвестных в получаемых системах в процессе решения должно монотонно уменьшаться (меняется число n). Следует также учитывать справедливость асимптотической оценки шенноновского типа о тривиальности расщеплений групп инерции почти всех функций в группах сдвигов ([3], теорема 5).

Пример.

Пусть функция от трех переменных над полем

$$\text{GF}(2^5) = \text{GF}(2)[x]/x^5 + x^2 + 1$$

задана многочленом

$$f(x_1, \dots, x_n) = x_1^4 x_2^5 + x_1^4 x_2^4 x_3^1 + x_2^4 x_3^3 + x_1^4 x_2 x_3^2 + x_1^4 x_3^3 + x_1^4 x_2^4 x_3^3 + x_2^5 x_3^2.$$

Все одночлены этого многочлена имеют степень нелинейности 3.

Сначала найдем группу $(H_3)_f^{(1)}$. Подпространство W_1 состоит из векторов $x = (x_1, x_2, x_3) \in \text{GF}(2^5)^3$, являющихся решениями системы уравнений

$$\begin{cases} a_2 + a_3 + a_3^2 = 0, \\ a_1^4 + a_3^2 = 0, \\ a_2^4 + a_3^2 = 0, \\ a_1^4 + a_2 + a_3 = 0, \\ a_1^4 + a_2^4 = 0, \\ a_2 + a_2^4 + a_3 = 0, \end{cases}$$

которая получается приравниванием к нулю коэффициентов многочлена Жегалкина левой части уравнения $\Delta_a f(x) = 0$ при одночленах степени нелинейности 2. Поскольку последние три уравнения являются следствиями трех первых, то достаточно решить систему

$$\begin{cases} a_2 + a_3 + a_3^2 = 0, \\ a_1^4 + a_3^2 = 0, \\ a_2^4 + a_3^2 = 0. \end{cases} \quad (9)$$

Воспользуемся изложенным выше методом. Выберем базис

$$\{1, \theta, \theta^2, \theta^3, \theta^4\},$$

где θ — корень неприводимого многочлена $x^5 + x^2 + 1$ над полем $\text{GF}(2)$. Пусть линейному многочлену $l_i(x) = x^{2^i}$ соответствует матрица C_i , где $i \in \{0, 1, 2\}$.

Непосредственной проверкой убеждаемся, что

$$C_0 = E, \quad C_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Тогда система (9) имеет вид

$$\begin{pmatrix} x_1^{(1)}, \dots, x_1^{(5)}, x_2^{(1)}, \dots, x_2^{(5)}, x_3^{(1)}, \dots, x_3^{(5)} \end{pmatrix} \begin{pmatrix} 0 & C_2 & 0 \\ E & 0 & C_2 \\ C_1 + C_2 & C_1 & C_1 \end{pmatrix} = (0, \dots, 0).$$

Решая ее, находим единственное ненулевое решение

$$\begin{pmatrix} x_1^{(1)}, \dots, x_1^{(5)}, x_2^{(1)}, \dots, x_2^{(5)}, x_3^{(1)}, \dots, x_3^{(5)} \end{pmatrix} = (00101, 00101, 01001).$$

Таким образом, $W_1 = \{0, a\}$, где $a = (\theta^2 + \theta^4, \theta^2 + \theta^4, \theta + \theta^4)$.

Подставляя найденный вектор в уравнение $\Delta_a f(x) = 0$, убеждаемся, что

$$W_0 = W_{-1} = \{0\}.$$

Окончательно получаем

$$\begin{aligned} |(H_3)_f^{(1)}| &= 2, \\ |(H_3)_f^{(0)}| &= |(H_3)_f| = 1. \end{aligned}$$

ЛИТЕРАТУРА

1. Черемушкин А. В. Аффинная эквивалентность и ее применение при изучении свойств дискретных функций (обзор результатов) // Материалы Междунар. научн. конф. по проблемам безопасности и противодействия терроризму. Интеллектуальный центр МГУ. (2–3 ноября 2005 г.) М.: МЦМНО, 2006. С. 103–130.
2. Лиддл Р., Нидеррайтер Г. Конечные поля. Т. 1, 2. М.: Мир, 1988. 818 с.
3. Черемушкин А. В. Некоторые асимптотические оценки для класса сильно зависимых функций // Вестник Томского госуниверситета. Приложение. 2006. № 17. С. 87–94.