ром неверно предполагалось, что для каждой APN-функции F такой класс состоит только из функций $F(x \oplus c) \oplus d$, где c, d пробегают $\mathbb{F}_2^n$. Однако найдены примеры квадратичных функций F от 4 переменных, для которых существуют линейные функции L, прибавление которых к исходной функции F сохраняет множества значений производных по всем направлениям, но при этом $F \oplus L$ не лежит в классе $\{F(x \oplus c) \oplus d : c, d \in \mathbb{F}_2^n\}$. Например, в качестве F можно выбрать APN-функцию $F(x_1, x_2, x_3, x_4) = (x_1x_2,\ x_1x_3 \oplus x_2x_4,\ x_2x_3 \oplus x_1x_4 \oplus x_2x_4,\ x_3x_4)$, а в качестве линейной следующую: $L(x_1, x_2, x_3, x_4) = (x_1 \oplus x_2,\ x_2 \oplus x_3,\ x_2,\ x_3 \oplus x_4)$. Тогда для любого ненулевого $a \in \mathbb{F}_2^4$ верно $B_a(F) = B_a(F \oplus L)$.

ЛИТЕРАТУРА

1. *Городилова А. А.* Характеризация APN-функций через подфункции // Прикладная дискретная математика. Приложение. 2014. № 7. С. 15–16.
2. *Туэкилин М. Э.* Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3. С. 14–20.
3. *Carlet C.* Open questions on nonlinearity and on APN functions // LNCS. 2015. V. 9061. P. 83–107.

УДК 512.552.18 DOI 10.17223/2226308X/8/10

ИССЛЕДОВАНИЕ ГРУППЫ БИЕКТИВНЫХ ДИФФЕРЕНЦИРУЕМЫХ ПО МОДУЛЮ p^n ФУНКЦИЙ

А. С. Ивачев

Описана с точностью до изоморфизма группа биективных дифференцируемых по модулю p^n функций, предложен способ поиска сопрягающего элемента в этой группе с помощью решения системы линейных уравнений над $\mathbb{Z}_p$, а также предложен способ генерации транзитивных функций с помощью биективных дифференцируемых по модулю p^n функций путём сопряжения функции $f(x) = x + 1$ биективными функциями.

Ключевые слова: *дифференцируемая по модулю p^n функция, биективная функция, транзитивная функция, сопряжение.*

Генерация последовательностей больших периодов, состоящих из элементов конечного кольца, является важной задачей в криптографии. Для генерации последовательности может использоваться следующая рекуррентная формула:

$$x_{i+1} = f(x_i), i = 1, 2, \ldots,$$

где f — некоторая функция над кольцом $\mathbb{Z}_{p^n}$.

Возникает проблема выбора f, такой, чтобы она легко вычислялась и генерировала последовательность $x_1x_2\ldots$ максимального периода p^n.

Как вариант выбора таких f в [1] предложены и исследованы дифференцируемые по модулю p^n функции, в том числе те из них, которые являются биективными и транзитивными. В частности, построены критерии биективности и транзитивности и получена формула для вычисления обратных биективных дифференцируемых по модулю p^n функций.

В данной работе проведено более глубокое изучение биективных дифференцируемых функций, а также основных задач, в которых данные функции могут быть применимы.

Напомним основные определения и утверждения, связанные с дифференцируемыми по модулю функциями.

Определение 1. Любая функция $f : \mathbb{Z}_p \to \mathbb{Z}_p$ является дифференцируемой функцией по модулю p. Функция $f : \mathbb{Z}_{p^n} \to \mathbb{Z}_{p^n}$ называется дифференцируемой по модулю p^n $(n > 1)$, если:

1) $f \bmod p^i$ — дифференцируемая по модулю p^i функция, $i = 1, \ldots, n-1$;
2) $f(x + ap^{n-1}) = f(x) + ap^{n-1}f'(x) \pmod{p^n}$, где f' — некоторая функция из $\mathbb{Z}_{p^n}$ в $\mathbb{Z}_{p^n}$. Функция f' называется производной функции f по модулю p^n.

Класс дифференцируемых функций обозначается D_n.

Пусть

$A_n = \{f : f \in D_n \wedge f_{n-1}(x) = 0\}$;
$B_n = \{f : f(x + ap^{n-1}) \equiv f(x) \pmod{p^n} \wedge f(x) \equiv 0 \pmod{p^{n-1}}\}$;
$C_n = \{f : f(x) = x_{n-1}p^{n-1}h'(x)$, где h' — производная некоторой функции из $D_n\}$.

Утверждение 1 [1]. Для любой функции f из D_n существует единственная тройка (f_A, f_B, f_C), где $f_A \in A_n$, $f_B \in B_n$, $f_C \in C_n$, такая, что $f(x) = f_A(x) + f_B(x) + f_C(x)$. Обратно, для каждой тройки (f_A, f_B, f_C), где $f_A \in A_n$, $f_B \in B_n$, $f_C \in C_n$, существует функция f из D_n, такая, что $f(x) = f_A(x) + f_B(x) + f_C(x)$.

Определение 2. Дифференцируемая по модулю p^n функция f называется обратимой (или биективной), если существует функция g, такая, что $g(f(x)) = x$. Функция g называется обратной для функции f.

Определение 3. Дифференцируемая по модулю p^n функция называется транзитивной, если она индуцирует одноцикловую подстановку на $\mathbb{Z}_{p^n}$.

Будем обозначать группу биективных дифференцируемых по модулю p^n функций с композицией в качестве операции как Bi_n. Пусть отображение $\pi_n : Bi_n \to Bi_{n-1}$ определяется как $\pi_n(f) = f \bmod p^{n-1}$. Очевидно, что это гомоморфизм с ядром

$$\operatorname{Ker}\pi_n = \{f : f(x) = x_0 + x_1p + \ldots + x_{n-2}p^{n-2} + f_B(x) + f'(x)x_{n-1}p^{n-1}, f_B \in B_n\}.$$

Ядро $\operatorname{Ker}\pi_n$ является группой относительно композиции функций в нем. В дальнейшем эта группа обозначается IB_n.

Пусть $\mathbb{L}_p = \langle \{f : \mathbb{Z}_p \to \mathbb{Z}_p : f(x) = ax + p, a \neq 0\}, \circ \rangle$.

Теорема 1.

$$Bi_n \simeq Bi_{n-1} \rtimes IB_n \simeq Bi_{n-1} \rtimes \bigoplus_{i=1}^{p^{n-1}} \mathbb{L}_p,$$

где при композиции функций в Bi_n компонента $\hat{f}$ из Bi_{n-1} переставляет функции f в IB_n по следующему закону:

$$\phi_{\hat{f}}(f)(x) = x_0 + x_1p + \ldots + x_{n-2}p^{n-2} + f_B(\hat{f_A}(x)) + f'(\hat{f_A}(x))x_{n-1}p^{n-1},$$

а именно: в сумме $\bigoplus_{i=1}^{p^{n-1}} \mathbb{L}_p$ слагаемое $ax + b$ с номером i ставится на место слагаемого $a^{\hat{f_A}}x + b^{\hat{f_A}}$ с номером $\hat{f_A}(i)$.

Здесь и далее если слагаемое $ax+b$ суммы $\bigoplus\limits_{i=1}^{p^{n-1}} \mathbb{L}_p$ имеет номер i и $f_A \in A_n$, то через $a^{f_A}x + b^{f_A}$ обозначается слагаемое этой суммы с номером $f_A(i)$.

Рассмотрим следующее равенство:

$$u = f^{-1} \circ v \circ f, \tag{1}$$

где $f, v, u \in Bi_n$. Оно фигурирует при рассмотрении следующих задач:

— поиск сопрягающего элемента;
— генерация транзитивных функций с помощью биективных.

Задача поиска сопрягающего элемента — это решение функционального уравнения, которое задаётся равенством (1) при известных u и v и неизвестном f. Искать сопрягающий элемент можно с помощью теоремы 1. Используя равенство

$$Bi_n \simeq Bi_{n-1} \rtimes \bigoplus_{i=1}^{p^{n-1}} \mathbb{L}_p,$$

можно проводить вычисления во второй части полупрямого произведения, если они уже проведены по первой. В $\mathbb{L}_p$ содержатся функции вида $ax+b$, $a \neq 0$. Соответственно, при решении уравнения (1) для каждого слагаемого суммы $\bigoplus\limits_{i=1}^{p^{n-1}} \mathbb{L}_p$ выполняется выражение

$$v_1 x + v_2 = (f_1^{u_A \circ f_A})^{-1}(u_1^{f_A}(f_1 x + f_2) + u_2^{f_A}) - (f_1^{u_A \circ f_A})^{-1} f_2^{u_A \circ f_A},$$

которое упрощается в систему

$$\begin{cases} v_1 f_1^{u_A \circ f_A} - u_1^{f_A} f_1 = 0, \\ v_2 f_1^{u_A \circ f_A} - u_2^{f_A} + f_2^{u_A \circ f_A} - u_1^{f_A} f_2 = 0. \end{cases}$$

Объединив эти системы для всех слагаемых, получим систему из $2p^{n-1}$ уравнений. Отметим, что она является линейной.

Получившуюся систему можно разбить на две части, одна — только из уравнений, в которых отсутствуют f_2, вторая — из уравнений, в которых f_2 присутствуют, и решать сначала первую, а затем вторую. Матрица получившейся системы представляет собой сумму перестановочных матриц, т. е. содержит большое число нулей, что может способствовать более быстрому её решению.

Другой задачей, в которой фигурируют биективные дифференцируемые по модулю p^n функции, является генерация транзитивных дифференцируемых по модулю p^n функций. Генерировать транзитивные функции с помощью равенства (1) можно, если положить v транзитивной функцией, и тогда u будет также транзитивной. Например, можно выбрать $v(x) = x + 1$, и тогда достаточно уметь генерировать биективные функции и вычислять значение обратной функции, чтобы вычислять u. Критерии биективности и формулу для вычисления обратной функции можно найти в [1]. Верна следующая

Теорема 2. Все транзитивные дифференцируемые по модулю p^n функции могут быть получены сопряжением функции $f(x) = x+1$ биективными дифференцируемыми по модулю p^n функциями.

Таким образом, пробегая по всем биективным функциям, можно предложенным способом получить все транзитивные функции.

Итак, для генерации последовательностей больших периодов биективные дифференцируемые по модулю p^n функции могут быть использованы как сопрягающие для транзитивных функций. Представляют интерес также статистические свойства таких последовательностей. Поэтому группа дифференцируемых по модулю p^n функций заслуживает внимания. Однако пока не описано представление, позволяющее эффективно вычислять данные функции, их реальное использование не практично. Поэтому в дальнейшем стоит задача поиска эффективного представления для функций из класса дифференцируемых по модулю p^n функций или из его подклассов. Предполагается, что данное представление можно получить для этих функций по модулю 2^n, используя элементарные операции, такие, как AND, XOR, RIGHT_SHIFT.

ЛИТЕРАТУРА

1. *Ивачев А. С.* Исследование класса дифференцируемых функций в кольцах классов вычетов по примарному модулю // Прикладная дискретная математика. Приложение. 2014. № 7. С. 19–22.

УДК 512.543.72 DOI 10.17223/2226308X/8/11

ОБРАЩЕНИЕ ДИФФЕРЕНЦИРУЕМЫХ ПЕРЕСТАНОВОК НАД ГРУППОЙ

А. В. Карпов

Вводится понятие дифференцируемой функции над группой с нормальным рядом, обобщающее понятие полиномиальной функции. Для абелевых, нильпотентных и разрешимых групп доказывается формула для нахождения обратной в смысле композиции перестановки к заданной дифференцируемой перестановке.

Ключевые слова: *перестановка, полином над группой, дифференцируемая функция.*

Пусть задана группа $\mathbb{G}$ с нормальным рядом $\mathbb{G} = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_n = e$. Через Ψ обозначим множество функций, отображающих $\mathbb{G}$ в себя, которые действуют на факторах H_k/H_{k+1} ($k \in \{0, \ldots, n-1\}$) как эндоморфизмы.

Определение 1. Функция $f : \mathbb{G} \to \mathbb{G}$ называется *дифференцируемой* в точке $a \in \mathbb{G}$ относительно нормального ряда $\mathbb{G} = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_n = e$, если существует функция $\psi_{f,a} \in \Psi$, такая, что для любого члена нормального ряда H_k и любого элемента $h \in H_k$ выполняется равенство

$$f(a+h) \equiv f(a) + \psi_{f,a}(h) \pmod{H_{k+1}}.$$

Функция называется дифференцируемой, если она дифференцируема в каждой точке группы $\mathbb{G}$. Функция $\psi_{f,a}$ называется производной функции f в точке a.

В качестве примеров дифференцируемых функций можно привести следующие: полиномиальные функции над примарным кольцом вычетов $\mathbb{Z}_{p^n}$, где в качестве $\mathbb{G}$ выступает $(\mathbb{Z}_{p^n}, +)$, $H_k = p^k\mathbb{Z}_{p^n}$, $\psi_{f,a} = f'(a)$ и $\psi_{f,a}(h) = h * f'(a)$; полиномиальные вектор-функции, т. е. системы из m полиномов от m переменных с коэффициентами из $\mathbb{Z}_{p^n}$, где $\mathbb{G} = (\mathbb{Z}_{p^n}^m, +)$, $\psi_{f,a}$ совпадает с матрицей частных производных, вычисленных в точке a;