Утверждение 2. При любых $n \in \mathbb{N}$ и $\mathcal{L} \subseteq \{0, \ldots, m-1\}$ класс $\mathcal{L}$-КЛР-функций $\mathcal{CLS}^{\mathcal{L}}_{p^m}(n)$ является замкнутым, то есть $[\mathcal{CLS}^{\mathcal{L}}_{p^m}(n)] = \mathcal{CLS}^{\mathcal{L}}_{p^m}(n)$.

Утверждение 3. При любом $n \in \mathbb{N}$ класс квази-ВКП-функций $\mathcal{QCP}_{p^m}(n)$ является замкнутым, то есть $[\mathcal{QCP}_{p^m}(n)] = \mathcal{QCP}_{p^m}(n)$.

Последние два утверждения приводят к интересному результату. При $m \geqslant 3$ в соответствии с теоремой 2 имеем цепочку включений: $\mathcal{P}_{p^m}(n) \subsetneq \mathcal{CP}_{p^m}(n) \subseteq \mathcal{QCP}_{p^m}(n) \subsetneq \subsetneq \mathcal{CLS}^{\{1,\ldots,m-1\}}_{p^m}(n)$. При этом в ней классы $\mathcal{P}_{p^m}(n)$, $\mathcal{QCP}_{p^m}(n)$, $\mathcal{CLS}^{\{1,\ldots,m-1\}}_{p^m}(n)$ являются замкнутыми и не равными друг другу.

Все четыре рассматриваемых класса $\mathcal{P}_{p^m}(n)$, $\mathcal{CP}_{p^m}(n)$, $\mathcal{QCP}_{p^m}(n)$, $\mathcal{CLS}^{\{1,\ldots,m-1\}}_{p^m}(n)$ обладают тем свойством, что системы уравнений (1), порождённые одним из них (т. е. системы, левые части которых $f_i(\mathbf{x})$ принадлежат ему), могут быть решены методом покоординатной линеаризации. Данный метод на самом деле является обобщением метода, предложенного в работах А. А. Нечаева и Д. А. Михайлова для класса полиномиальных функций. Для случая примарных колец вычетов $\mathbb{Z}_{2^m}$ его изложение опубликовано в работах [2, 3].

ЛИТЕРАТУРА

1. *Михайлов Д. А., Нечаев А. А.* Решение системы полиномиальных уравнений над кольцом Галуа — Эйзенштейна с помощью канонической системы образующих полиномиального идеала // Дискретная математика. 2004. Т. 1. Вып. 1. С. 21–51.
2. *Заец М. В., Никонов В. Г., Шишков А. Б.* Функции с вариационно-координатной полиномиальностью и их свойства // Открытое образование. 2012. № 3. С. 57–61.
3. *Заец М. В., Никонов В. Г., Шишков А. Б.* Класс функций с вариационно-координатной полиномиальностью над кольцом $\mathbb{Z}_{2^m}$ и его обобщение // Матем. вопросы криптографии. 2013. Т. 4. Вып. 3. С. 19–45.

УДК 512.552.18

ИССЛЕДОВАНИЕ КЛАССА ДИФФЕРЕНЦИРУЕМЫХ ФУНКЦИЙ В КОЛЬЦАХ КЛАССОВ ВЫЧЕТОВ ПО ПРИМАРНОМУ МОДУЛЮ

А. С. Ивачев

Для класса D_n дифференцируемых по модулю p^n функций, являющегося обобщением класса полиномиальных функций, найдены подмножества функций A_n, B_n, C_n, такие, что для каждой функции из D_n существует единственное представление через функции подмножеств A_n, B_n, C_n. С помощью этого представления получены число всех функций, число биективных функций и число транзитивных функций класса D_n. Из полученных мощностных соотношений следует, что в множество транзитивных дифференцируемых по модулю p^2 функций входят только полиномиальные функции, однако при подъёме модуля множество дифференцируемых транзитивных функций начинает отличаться от множества транзитивных полиномиальных функций. Показано, что для обратимости функции из D_n необходимым и достаточным условием является её обратимость по модулю p и неравенство нулю производных по всем модулямю p^i, $i = 2, \ldots, n$. Получена рекуррентная формула для вычисления обратной функции. Найдены условия транзитивности функций, из которых следует, что из любой транзитивной дифференцируемой по модулю p^{n-1} функции можно построить транзитивную дифференцируемую по модулю p^n функцию, совпадающую с первой по модулю p^{n-1}.

Ключевые слова: *рекуррентная последовательность, дифферерениируемая функция, обратная функция, биективная функция, транзитивная функция.*

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

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

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

Возникает проблема выбора такой функции f, чтобы она легко вычислялась и генерировала последовательность максимального периода p^n.

Над кольцом $\mathbb{Z}_{p^n}$ известен класс полиномиальных функций. Существуют функции этого класса, соответствующие указанным требованиям, однако их доля среди множества всех функций над $\mathbb{Z}_{p^n}$ мала. Так появляется задача изучения новых классов функций над $\mathbb{Z}_{p^n}$. В данной работе рассматривается класс дифференцируемых по модулю p^n функций. Подобный класс был определён в [1].

Для функции $f : \mathbb{Z}_{p^n} \to \mathbb{Z}_{p^n}$ будем обозначать $f \bmod p^i$ функцию g из $\mathbb{Z}_{p^i}$ в $\mathbb{Z}_{p^i}$, такую, что $g(x) = f(x) \bmod p^i$, подразумевая, что g определена корректно.

Определение 1. Любая функция $f : \mathbb{Z}_p \to \mathbb{Z}_p$ является дифференцируемой 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.

Класс дифференцируемых функций включает в себя класс полиномиальных функций и замкнут относительно сложения, умножения, операции композиции функций. Каждую функцию f над $\mathbb{Z}_{p^n}$ можно представить в виде

$$f(x) = \sum_{i=0}^{n-1} f_i(x)p^i,$$

где f_i принимают значение в множестве $\{0, 1, \ldots, p-1\}$.

Такое представление назовём координатным представлением функции f, а f_i — координатными функциями, или координатами функции f. Координатные функции f_i дифференцируемой функции f обладают следующим свойством:

$$f_i(x) = f_i(x + ap^{n-1}), \quad i = 0, \ldots, n-2.$$

Из определения 1 следует, что функция f' тогда и только тогда является производной некоторой функции, когда её первая координата не зависит от последней координаты x, то есть $f'(x + ap^{n-1}) \equiv f'(x) \pmod{p}$ для любого a из $\mathbb{Z}_{p^n}$.

Определим следующие множества:

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

Из определения множеств A_n, B_n, C_n следует, что они являются подмножествами D_n. Для функций из данных множеств справедливо следующее утверждение.

Утверждение 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), $f_A \in A_n$, $f_B \in B_n$, $f_C \in C_n$, существует f из D_n, такая, что $f(x) = f_A(x) + f_B(x) + f_C(x)$.

Следствие 1. $|D_n| = |A_n| \cdot |B_n| \cdot |C_n|$.

Между A_n и D_{n-1} существует биекция π_n, такая, что $\pi_n(f) = f \bmod p^{n-1}$, и соответственно $|D_{n-1}| = |A_n|$.

Следствие 2. Число дифференцируемых функций равно $p^{p+2p(p^{n-1}-1)/(p-1)}$.

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.

Обратная функция для дифференцируемой биективной функции также является дифференцируемой. Следующее утверждение представляет собой критерий обратимости функции.

Утверждение 2. Пусть $f \in D_n$. Тогда f обратима тогда и только тогда, когда $f \bmod p$ обратима и производные функций $f \bmod p^i$, где $i = 2, \ldots, n$, не обращаются в 0 при любом значении x.

Следствие 3. Число биективных дифференцируемых функций равно

$$p\,!((p-1)p)^{p(p^{n-1}-1)/(p-1)}.$$

В следующем утверждении приведена формула для обратной функции:

Утверждение 3. Пусть f — обратимая дифференцируемая функция и g — обратная к f. Тогда справедлива следующая формула:

$$g(x) = g(x) \bmod p^{n-1} - g'(x)(f(g(x) \bmod p^{n-1}) - f(g(x) \bmod p^{n-1}) \bmod p^{n-1} - x_{n-1}p^{n-1}).$$

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

Введём следующие обозначения:

$f^{[k]}(x) = \underbrace{f(f(\cdots f(x)\cdots))}_{k \text{ раз}}$,

$a(n, m, f_A, f', x) = \prod\limits_{k=1}^{mp^n} f'(f_A^{[mp^n-k]}(x)) \pmod p$,

$b(n, m, f_A, f_B, f', x) = \sum\limits_{k=1}^{mp^n} f_B(f_A^{[mp^n-k]}(x)) \prod\limits_{j=1}^{k-1} f'(f_A^{[mp^n-j]}(x))$.

Утверждение 4. Пусть $f \in D_n$. Тогда f транзитивна тогда и только тогда, когда $f \bmod p^{n-1}$ транзитивна в D_{n-1}, $a(n-1, 1, f_A, f', 0) = 1$ и $b(n-1, 1, f_A, f_B, f', 0) \neq 0$.

Следствие 4. Число транзитивных дифференцируемых функций равно

$$(p-1)\,!(p-1)^{p(p^{n-1}-1)/(p-1)}p^{p(p^{n-1}-1)/(p-1)-n+1}.$$

Транзитивные дифференцируемые функции составляют долю $1/p^n$ в множестве биективных дифференцируемых функций. По модулю p^2 все биективные, а соответственно и транзитивные дифференцируемые функции являются полиномиальными вследствие формул для числа биективных и транзитивных полиномиальных функций, приведённых в [2]. Однако производная дифференцируемой функции зависит от $n-1$ первых координат x и при подъёме модуля в общем случае производная по большему модулю не зависит от производных по меньшему модулю, в то время как производная полиномиальной функции зависит только от первой координаты и при подъёме модуля не изменяется. Таким образом, по модулю p^n, $n>2$, число транзитивных дифференцируемых функций больше, чем число транзитивных полиномиальных функций. Однако ещё не известно представлений для дифференцируемых функций, позволяющих эффективно вычислять их. Таким образом, появляется задача поиска таких представлений для функций класса D_n. Если такие представления будут найдены, то дифференцируемые функции могут быть использованы для генерации последовательностей элементов из $\mathbb{Z}_{p^n}$ по формуле (1).

ЛИТЕРАТУРА

1. *Анашин В. С.* Равномерно распределенные последовательности целых p-адических чисел // Дискретная математика. 2002. №14:4. С. 3–64.
2. *Ларин М. В.* Транзитивные полиномиальные преобразования колец вычетов // Дискретная математика. 2002. №14:2. С. 20–32.

УДК 519.7

ВЕРХНЯЯ ОЦЕНКА ЧИСЛА БЕНТ-ФУНКЦИЙ НА РАССТОЯНИИ 2^k ОТ ПРОИЗВОЛЬНОЙ БЕНТ-ФУНКЦИИ ОТ $2k$ ПЕРЕМЕННЫХ[1]

Н. А. Коломеец

Получена верхняя оценка числа бент-функций на расстоянии 2^k от произвольной бент-функции от $2k$ переменных. Установлено, что она достигается только для квадратичных бент-функций. Введено понятие полной аффинной расщепляемости булевой функции. Доказано, что полностью аффинно расщепляемыми могут быть только аффинные и квадратичные функции.

Ключевые слова: *булевы функции, бент-функции, квадратичные бент-функции.*

Функция $f:\mathbb{Z}_2^n\to\mathbb{Z}_2$ называется *булевой функцией* от n переменных. Булева функция называется *аффинной*, если степень её алгебраической нормальной формы не превосходит 1, и *квадратичной*, если степень равна 2. Заметим, что любая аффинная функция от n переменных представима в виде $f(x)=\langle a,x\rangle\oplus c$, где $a\in\mathbb{Z}_2^n$; $c\in\mathbb{Z}_2$; $\langle a,x\rangle=a_1x_1\oplus\ldots\oplus a_nx_n$. *Расстояние* между двумя булевыми функциями от n переменных — расстояние Хэмминга между векторами их значений. *Бент-функция* — булева функция от чётного числа переменных, находящаяся на максимально возможном расстоянии от множества всех аффинных функций. Подробнее о бент-функциях можно узнать в работах [1, 2]. Множество $s\oplus D=\{s\oplus x : x\in D\}$ называется *сдвигом* множества $D\subseteq\mathbb{Z}_2^n$, $s\in\mathbb{Z}_2^n$. *Аффинное подпространство* $\mathbb{Z}_2^n$ — сдвиг некоторого линейного подпространства $\mathbb{Z}_2^n$. *Размерностью* аффинного подпространства называется размер-

[1]Работа поддержана грантом НШ-1939.2014.1 Президента России для ведущих научных школ.