(*) для всех $x, y, a \in \mathbb{Z}_2^n$, $a \neq 0$, хотя бы одно из равенств $D_aF(x) = D_aG(y)$ и $D_af(x) = D_ag(y)$ нарушается;

(**) для всех $x, y, a \in \mathbb{Z}_2^n$, $a \neq 0$, $x \neq y, y \oplus a$, хотя бы одно из равенств $D_aH(x) = D_aH(y)$ и $D_ah(x) = D_ah(y)$ нарушается, где $H = F$ и $h = f$, либо $H = G$ и $h = g$.

Получена следующая теорема о характеризации APN-функций через набор подфункций, обобщающая результат теоремы 3 из [3].

Теорема 1. Векторная функция S от n переменных — APN-функция тогда и только тогда, когда набор её подфункций F, G, f, g является допустимым и каждая из векторных функций F и G либо APN-функция, либо имеет порядок дифференциальной равномерности равный 4.

При малом числе переменных получена следующая характеризация APN-функций от n переменных через векторные подфункции F и G от $n-1$ переменных:

	$n = 2$	$n = 3$	$n = 4$
Количество всех APN-функций от n пер.	192	668 128	18 940 805 775 360
F, G — APN-функции	192	589 824 = 6/7 от всех	4 419 521 347 584 = 7/30 от всех
F, G — порядка диф. рав. 4	—	98 304 = 1/7 от всех	11 995 843 657 728 = 19/30 от всех
Одна функция — APN, другая — порядка диф. рав. 4	—	—	2 525 440 770 048 = 4/30 от всех

Вычисления для случая $n = 4$ проводились на кластере НКС-30Т ССКЦ СО РАН.

ЛИТЕРАТУРА

1. *Nyberg K.* Differentially uniform mappings for cryptography // Eurocrypt 1993. LNCS. 1994. V. 765. P. 55–64.
2. *Тужилин М. Э.* Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3. С. 14–20.
3. *Фролова А. А.* Итеративная конструкция APN-функций // Прикладная дискретная математика. Приложение. 2013. № 6. С. 24–25.

УДК 519.716.32+519.854

КЛАССИФИКАЦИЯ ФУНКЦИЙ НАД ПРИМАРНЫМ КОЛЬЦОМ ВЫЧЕТОВ В СВЯЗИ С МЕТОДОМ ПОКООРДИНАТНОЙ ЛИНЕАРИЗАЦИИ

М. В. Заец

Известно, что для решения систем полиномиальных уравнений над примарным кольцом вычетов можно применять метод покоординатной линеаризации. Рассматривается классификация функций над примарным кольцом вычетов, порождающих системы уравнений, для которых также применим указанный метод. Класс полиномиальных функций расширяется классом вариационно-координатно-полиномиальных функций (ВКП-функций), который, в свою очередь, расширяется классом квази-ВКП-функций и классом координатно-линейно разрешимых функций. Описываются свойства введённых классов функций.

Ключевые слова: *полиномиальные функции, вариационно-координатно-полиномиальные функции, ВКП-функции, квази-ВКП-функции, координатно-линейно разрешимые функции, метод покоординатной линеаризации, системы уравнений.*

Исследование систем уравнений над кольцом $\mathbb{Z}_{p^m}$

$$\begin{cases} f_1(\mathbf{x}) = y_1, \\ \quad\vdots \\ f_t(\mathbf{x}) = y_l, \end{cases} \tag{1}$$

позволяет выделить некоторые классы функций, для которых система (1) обладает свойством внутренней структурности.

Любой элемент a примарного кольца вычетов $\mathbb{Z}_{p^m}$, где $m \in \mathbb{N}$, $m > 1$ и p простое, можно однозначно представить в виде

$$a = a^{(0)} + p \cdot a^{(1)} + \cdots + p^{m-1} \cdot a^{(m-1)},$$

где $a^{(j)} \in \mathcal{B} = \{0, \ldots, p-1\}$, называемом разложением элемента a в p-ичном координатном множестве $\mathcal{B}$. Отображения

$$\gamma_j : \mathbb{Z}_{p^m} \to \mathcal{B}, \quad \gamma_j(a) = a^{(j)}, \quad j = 0, \ldots, m-1,$$

называются координатными функциями в координатном множестве $\mathcal{B}$, а элементы $a^{(j)} = \gamma_j(a) \in \mathcal{B}$ — координатами j-го порядка элемента a в координатном множестве $\mathcal{B}$. Если при этом ввести на $\mathcal{B}$ операции сложения $\oplus$ и умножения $\otimes$ по правилу

$$a \oplus b = \gamma_0(a + b), \quad a \otimes b = \gamma_0(a \cdot b), \quad a, b \in \mathcal{B},$$

то алгебра $(\mathcal{B}, \oplus, \otimes) \cong \mathrm{GF}(p)$ будет являться полем из p элементов. В работе рассмотрены классы функций над примарным кольцом вычетов $\mathbb{Z}_{p^m}$, обобщающие в некотором смысле класс $\mathcal{P}_{p^m}(n)$ — полиномиальных функций над данным кольцом. В [1] в общем случае для GE-колец (колец Галуа — Эйзентштейна, т. е. конечных коммутативных цепных колец) показано, что системы полиномиальных уравнений могут быть решены методом покоординатной линеаризации. Данный метод заключается в последовательном нахождении координат неизвестных переменных. Сначала находятся младшие координаты неизвестных переменных путём решения исходной системы над полем $\mathcal{B}$, приведённой по модулю p. Затем находятся остальные координаты путём многократного решения $m-1$ систем линейных уравнений над полем $\mathcal{B}$. Показано, что данным свойством обладают не только системы полиномиальных уравнений.

Определение 1. Для функции $f(\mathbf{x})\colon \mathbb{Z}_{p^m}^n \to \mathbb{Z}_{p^m}$ и $j \in \{0, \ldots, m-1\}$ отображение $\gamma_j f\colon \mathbb{Z}_{p^m}^n \to \mathcal{B}$, определяемое по правилу

$$\gamma_j f(\alpha) = \gamma_j(f(\alpha))$$

для всех $\alpha \in \mathbb{Z}_{p^m}^n$, будем называть её j-й координатной функцией, или j-м координатным отображением.

Определение 2. Функцию $f(\mathbf{x})\colon \mathbb{Z}_{p^m}^n \to \mathbb{Z}_{p^m}$ назовём вариационно-координатно-полиномиальной (или ВКП-функцией), если для любого $j \in \{0, \ldots, m-1\}$ существует полиномиальная функция $p_j(\mathbf{x}) \in \mathcal{P}_{p^m}(n)$, j-я координатная функция которой совпадает с j-й координатной функцией функции $f(\mathbf{x})$, т. е. выполняется равенство

$$\gamma_j f(\mathbf{x}) = \gamma_j p_j(\mathbf{x}), \quad j = 0, \ldots, m-1.$$

Определение 3. Функцию $f(\mathbf{x})\colon \mathbb{Z}_{p^m}^n \to \mathbb{Z}_{p^m}$ назовем квазивариационно-координатно-полиномиальной (или квази-ВКП-функцией), если выполнены условия:

1) $\gamma_0 f(\mathbf{x}) = \gamma_0 f(\mathbf{x}^{(0)}) = g_0(\mathbf{x}^{(0)})$, $g_0\colon \mathcal{B}^n \to \mathcal{B}$;
2) для любого $j \in \{0, \ldots, m-1\}$ существуют функции $g_{ji}\colon \mathcal{B}^n \to \mathcal{B}$, $g_j\colon \mathcal{B}^{jn} \to \mathcal{B}$, $i = 1, \ldots, n$, над полем $\mathcal{B}$, такие, что справедливо равенство

$$\gamma_j f(\mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(j)}) = \sum_{i=1}^{n} g_{ji}(\mathbf{x}^{(0)}) \otimes x_i^{(j)} \oplus g_j(\mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(j-1)}).$$

Определение 4. Функцию $f(\mathbf{x})\colon \mathbb{Z}_{p^m}^n \to \mathbb{Z}_{p^m}$ назовем координатно $\mathcal{L}$-линейно разрешимой (или $\mathcal{L}$-КЛР-функцией), где $\mathcal{L} \subseteq \{0, \ldots, m-1\}$, если $\gamma_j f(\mathbf{x}) = \gamma_j f(\mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(j)})$, $j = 0, \ldots, m-1$, и при любом $j \in \mathcal{L}$, $j \neq 0$, существуют такие функции $g_{ji}, g_j : \mathcal{B}^{nj} \to \mathcal{B}$, $i = 1, \ldots, n$, что

$$\gamma_j f(\mathbf{x}) = \sum_{i=1}^{n} g_{ji}(\mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(j-1)}) \otimes x_i^{(j)} \oplus g_j(\mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(j-1)}),$$

и при $0 \in \mathcal{L}$ существуют такие $g_{0i}, g_0 \in \mathcal{B}$, $i = 1, \ldots, n$, что

$$\gamma_0 f(\mathbf{x}) = \sum_{i=1}^{n} g_{0i} \otimes x_i^{(0)} \oplus g_0.$$

Класс всех ВКП-функций от n переменных над $\mathbb{Z}_{p^m}$ обозначим через $\mathcal{CP}_{p^m}(n)$. Класс всех квази-ВКП-функций от n переменных над кольцом $\mathbb{Z}_{p^m}$ обозначим $\mathcal{QCP}_{p^m}(n)$. При заданном подмножестве $\mathcal{L} \subseteq \{0, \ldots, m-1\}$ обозначим класс всех $\mathcal{L}$-КЛР-функций от n переменных над $\mathbb{Z}_{p^m}$ через $\mathcal{CLS}_{p^m}^{\mathcal{L}}(n)$. Обозначим через $\mathcal{D}_{p^m}(n)$ класс всех функций над $\mathbb{Z}_{p^m}$ от n переменных, сохраняющих отношение сравнимости по любому делителю p^m или, что то же самое, сохраняющих любую конгруэнцию кольца $\mathbb{Z}_{p^m}$. Соотношения между данными классами функций устанавливает следующее утверждение.

Утверждение 1. Если $\mathcal{L} \subseteq \{1, \ldots, m-1\}$, то справедлива цепочка включений

$$\mathcal{P}_{p^m}(n) \subseteq \mathcal{CP}_{p^m}(n) \subseteq \mathcal{QCP}_{p^m}(n) \subseteq \mathcal{CLS}_{p^m}^{\mathcal{L}}(n) \subseteq \mathcal{D}_{p^m}(n).$$

При этом если $\mathcal{L} \subsetneq \{1, \ldots, m-1\}$, то $\mathcal{QCP}_{p^m}(n) \subsetneq \mathcal{CLS}_{p^m}^{\mathcal{L}}(n)$.

Теорема 1. Пусть $\mathcal{L} = \{1, \ldots, m-1\}$, тогда справедливы утверждения:

1) верна цепочка равенств

$$\mathcal{P}_{p^2}(n) = \mathcal{CP}_{p^2}(n) = \mathcal{QCP}_{p^2}(n) = \mathcal{CLS}_{p^2}^{\mathcal{L}}(n);$$

2) при $m \geqslant 3$ верна цепочка включений

$$\mathcal{P}_{p^m}(n) \subsetneq \mathcal{CP}_{p^m}(n) \subseteq \mathcal{QCP}_{p^m}(n) \subsetneq \mathcal{CLS}_{p^m}^{\mathcal{L}}(n).$$

Теорема 2. Классы $\mathcal{CLS}_{p^m}^{\mathcal{L}}(n)$ и $\mathcal{D}_{p^m}(n)$ при $\mathcal{L} = \{1, \ldots, m-1\}$ совпадают тогда и только тогда, когда одновременно $p = 2$ и $n = 1$.

Следствие 1. Справедливы следующие равенства классов функций над $\mathbb{Z}_4$:

$$\mathcal{P}_4(1) = \mathcal{CP}_4(1) = \mathcal{QCP}_4(1) = \mathcal{CLS}_4^{\{1\}}(1) = \mathcal{D}_4(1).$$

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}.