ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

2014 Теоретические основы прикладной дискретной математики № 3(25)

DOI 10.17223/20710410/25/2

УДК 519.716.32+519.854

О КЛАССЕ ВАРИАЦИОННО-КООРДИНАТНО-ПОЛИНОМИАЛЬНЫХ ФУНКЦИЙ НАД ПРИМАРНЫМ КОЛЬЦОМ ВЫЧЕТОВ[1]

М. В. Заец

ФГУП НИИ «КВАНТ», г. Москва, Россия

E-mail: mirzaets@hotmail.com

Работа посвящена изучению нового класса функций над примарным кольцом вычетов, который получил название класса функций с вариационно-координатной полиномиальностью. Этот класс обобщает класс полиномиальных функций и наряду с ним обладает тем свойством, что системы уравнений, составленные из таких функций, могут быть решены методом покоординатной линеаризации.

Ключевые слова: *примарное кольцо вычетов, полиномиальные функции, формальные производные, системы уравнений, ВКП-функции.*

Введение

Известно, что системы полиномиальных уравнений над кольцом Галуа — Эйзенштейна (т. е. конечным коммутативным цепным кольцом) могут быть решены методом покоординатной линеаризации [1]. Частным случаем такого кольца является примарное кольцо вычетов $\mathbb{Z}_{p^m}$, $m \in \mathbb{N}$. Суть рассматриваемого метода над $\mathbb{Z}_{p^m}$ заключается в последовательном нахождении p-ичных координат неизвестных переменных, при этом нахождение $(i+1)$-х координат при известных координатах меньшего порядка сводится к решению системы линейных уравнений над полем $\mathrm{GF}(p)$. В работе [2] показано, что класс функций над кольцом вычетов $\mathbb{Z}_{2^m}$, обладающий таким свойством, шире класса полиномиальных при $m \geqslant 3$. Построенный класс назван классом «вариационно-координатно-полиномиальных функций» (ВКП-функций). Данная работа продолжает изучение ВКП-функций и обобщает результаты, полученные ранее в [2, 3], на произвольное кольцо вычетов $\mathbb{Z}_{p^m}$.

1. Свойства полиномиальных функций над $\mathbb{Z}_{p^m}$

Сформулируем и докажем некоторые свойства полиномиальных и треугольных функций над примарным кольцом вычетов, которые необходимы для описания свойств ВКП-функций. Напомним, что функция называется полиномиальной над кольцом вычетов $\mathbb{Z}_k$, $k > 1$, если она представима формулой над классом $\{x_1x_2, x_1+x_2, 1\}$, или, что то же самое, представима некоторым многочленом из $\mathbb{Z}_k[x_1, \ldots, x_n]$. Обозначим класс всех полиномиальных функций от $n \in \mathbb{N}$ переменных над кольцом $\mathbb{Z}_k$ через $\mathcal{P}_k(n)$. Договоримся функции от переменных $x_1, \ldots, x_n$ записывать кратко $f(\mathbf{x})$, класс всех функций от n переменных над кольцом вычетов $\mathbb{Z}_k$ обозначим $\mathcal{F}_k(n)$. При этом равенства $f(\mathbf{x}) = g(\mathbf{x})$ или сравнения вида $f(\mathbf{x}) \equiv g(\mathbf{x}) \pmod{p^j}$ будем понимать соответственно как равенство и сравнение, выполнимые при всех $\mathbf{x}$. Всюду далее считаем, если не оговорено иное, что m, n — произвольные натуральные числа и $m > 1$.

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

$$a = a^{(0)} + pa^{(1)} + \ldots + p^{m-1}a^{(m-1)},\ j = 0, \ldots, m-1,$$

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

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

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

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 $\mathcal{B}$. В частности, любой вектор $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}_{p^m}^n$ однозначно представляется в виде суммы

$$\mathbf{x} = \mathbf{x}^{(0)} + p\mathbf{x}^{(1)} + \ldots + p^{m-1}\mathbf{x}^{(m-1)},$$

где $\mathbf{x}^{(j)} = (x_1^{(j)}, \ldots, x_n^{(j)}) \in \mathcal{B}^n$. Если ввести на $\mathcal{B}$ операции сложения $\oplus$ и умножения $\otimes$ по правилу

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

то алгебра $(\mathcal{B}, \oplus, \otimes) \cong \mathbb{Z}_{p^m}/p\mathbb{Z}_{p^m} \cong \mathrm{GF}(p)$ будет являться полем из p элементов.

Определение 1. Для функции $f(\mathbf{x}) \in \mathcal{F}_{p^m}(n)$ 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*.

Другими словами, если $f(\mathbf{x}) \in \mathcal{F}_{p^m}(n)$, то она представима в виде суммы

$$f(\mathbf{x}) = \sum_{j=0}^{m-1} p^j \gamma_j f(\mathbf{x}).$$

При этом любую координатную функцию $\gamma_j f$, $j = 0, \ldots, m-1$, можно рассматривать в то же время как функцию $\gamma_j f \colon \mathcal{B}^{nm} \to \mathcal{B}$ от nm переменных над полем $\mathcal{B}$, в роли которых выступают координаты $\mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(m-1)}$, при этом в таком случае будем предполагать, что координаты переменных расположены в указанном порядке, т. е. $\gamma_j f = \gamma_j f(\mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(m-1)})$. А следовательно, любая такая координатная функция может быть представлена многочленом над полем $\mathcal{B}$ от указанных переменных [4].

Определение 2. Функцию $f(\mathbf{x}) \in \mathcal{F}_{p^m}(n)$ будем называть *T-функцией*, или *треугольной функцией*, если для любого $j \in \{0, \ldots, m-1\}$ её j-я координатная функция зависит только от координат переменных $\mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(j)}$, т. е. если $f(\mathbf{x})$ имеет вид

$$f(\mathbf{x}) = \sum_{i=0}^{m-1} p^j \gamma_j f(\mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(j)}).$$

Примерами треугольных функций над кольцом $\mathbb{Z}_{p^m}$ являются полиномиальные функции. Для объяснения данного факта потребуется ввести еще несколько определений.

Определение 3. Будем говорить, что наборы целых чисел $\alpha = (a_1, \ldots, a_n)$ и $\beta = (b_1, \ldots, b_n)$ *сравнимы по модулю* d (или $\alpha \equiv \beta \pmod{d}$), если $a_i \equiv b_i \pmod{d}$ для всех $i \in \{1, \ldots, n\}$.

Определение 4. Функция $f(\mathbf{x}) \in \mathcal{F}_{p^m}(n)$ *сохраняет отношение сравнимости по модулю* $d \mid p^m$, если на сравнимых по модулю d наборах она принимает сравнимые значения по модулю d.

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 $\mathbb{Z}_{p^m}$. Из простейших свойств сравнений следует, что любая полиномиальная функция $f(\mathbf{x}) \in \mathcal{P}_{p^m}(n)$ сохраняет отношение сравнимости по любому делителю p^m, и поэтому справедливо включение $\mathcal{P}_{p^m}(n) \subseteq \mathcal{D}_{p^m}(n)$.

Следующая теорема устанавливает связь между классом треугольных функций и классом $\mathcal{D}_{p^m}(n)$. Её доказательство несложно получить, используя работу [5].

Теорема 1. Пусть $f(\mathbf{x}) \in \mathcal{F}_{p^m}(n)$. Равносильны следующие утверждения:

1) $f(\mathbf{x}) \in \mathcal{D}_{p^m}(n)$;
2) $f(\mathbf{x})$ является Т-функцией.

Таким образом, классы треугольных функций и функций, сохраняющих отношение сравнимости по любому делителю p^m, совпадают. Отсюда следует, что полиномиальные функции являются треугольными.

Пусть $f(\mathbf{x}) \in \mathbb{Z}_{p^m}[x_1, \ldots, x_n]$. Полиномиальную вектор-функцию $\operatorname{grad} f(\mathbf{x}) = \left(\dfrac{\partial f}{\partial x_1}(\mathbf{x}), \ldots, \dfrac{\partial f}{\partial x_n}(\mathbf{x})\right)$ будем называть градиентом многочлена $f(\mathbf{x})$, где $\dfrac{\partial f}{\partial x_i}(\mathbf{x})$ — формальная частная производная многочлена $f(\mathbf{x})$ по переменной x_i, $i = 1, \ldots, n$. Следующая теорема является основной для дальнейших рассуждений.

Теорема 2 (формула Тейлора [1]). Для любого многочлена $f(\mathbf{x}) \in \mathbb{Z}_{p^m}[x_1, \ldots, x_n]$ и любых $j \in \{1, \ldots, m-1\}$, $\mathbf{h} = (h_1, \ldots, h_n) \in \mathbb{Z}_{p^m}^n$ справедливо сравнение

$$f(\mathbf{x} + p^j\mathbf{h}) \equiv f(\mathbf{x}) + p^j \operatorname{grad} f(\mathbf{x}) \cdot \mathbf{h} \pmod{p^{j+1}}, \tag{1}$$

где $\operatorname{grad} f(\mathbf{x}) \cdot \mathbf{h} = \sum\limits_{i=1}^{n} \dfrac{\partial f}{\partial x_i}(\mathbf{x}) h_i$.

Теорему 2 можно в некотором смысле уточнить. Пусть $\operatorname{grad} f(\mathbf{x})$ — градиент многочлена $f(\mathbf{x}) \in \mathbb{Z}_{p^m}[x_1, \ldots, x_n]$. Приведём каждую его компоненту (формальную частную производную) по модулю p. Тогда в силу свойств многочленов получим полиномиальную вектор-функцию над полем $\mathcal{B}$ от переменных $\mathbf{x}^{(0)}$:

$$\operatorname{grad} f(\mathbf{x}) \equiv \operatorname{grad} f(\mathbf{x}^{(0)}) \pmod{p}.$$

В дальнейшем будем её обозначать $\operatorname{grad} f(\mathbf{x}) \pmod{p}$. Докажем простое следствие.

Следствие 1. Для любого многочлена $f(\mathbf{x}) \in \mathbb{Z}_{p^m}[x_1, \ldots, x_n]$ и любых $j \in \{1, \ldots, m-1\}$, $\mathbf{h} = (h_1, \ldots, h_n) \in \mathbb{Z}_{p^m}^n$ справедливо сравнение

$$f(\mathbf{x} + p^j\mathbf{h}) \equiv f(\mathbf{x}) + p^j \operatorname{grad} f(\mathbf{x}^{(0)}) \cdot \mathbf{h}^{(0)} \pmod{p^{j+1}}, \tag{2}$$

где $\operatorname{grad} f(\mathbf{x}^{(0)}) \cdot \mathbf{h}^{(0)} = \sum\limits_{i=1}^{n} \dfrac{\partial f}{\partial x_i}(\mathbf{x}^{(0)}) h_i^{(0)}$.

Доказательство. Достаточно воспользоваться формулой 1 и тем, что $\dfrac{\partial f}{\partial x_i}(\mathbf{x})$ является также многочленом, а значит, $\dfrac{\partial f}{\partial x_i}(\mathbf{x}) h_i \equiv \dfrac{\partial f}{\partial x_i}(\mathbf{x}^{(0)}) h_i^{(0)} \pmod{p}$, откуда и следует сравнение $p^j \operatorname{grad} f(\mathbf{x}) \cdot \mathbf{h} \equiv p^j \operatorname{grad} f(\mathbf{x}^{(0)}) \cdot \mathbf{h}^{(0)} \pmod{p^{j+1}}$. ■

Лемма 1. Если $a = x + p^j y$, где $x, y \in \mathbb{Z}_{p^m}$ и $j \in \{0, \ldots, m-1\}$, то

$$\gamma_j(a) = \gamma_j(x) \oplus \gamma_0(y).$$

Доказательство. Легко видеть, что
$\gamma_j(a) = \gamma_j(x + p^j y) = \gamma_j(x + p^j(\gamma_0(y) + p\gamma_1(y) + \ldots + p^{m-1}\gamma_{m-1}(y))) = \gamma_j(x) \oplus \gamma_0(y)$. ■

Теперь, если применить результаты леммы 1 к следствию 1, получим ещё одно

Следствие 2. Для любого многочлена $f(\mathbf{x}) \in \mathbb{Z}_{p^m}[x_1, \ldots, x_n]$ и любых $j \in \{1, \ldots, m-1\}$, $\mathbf{h} = (h_1, \ldots, h_n) \in \mathbb{Z}_{p^m}^n$ справедливо сравнение

$$\gamma_j f(\mathbf{x} + p^j \mathbf{h}) \equiv \gamma_j f(\mathbf{x}) + \operatorname{grad} f(\mathbf{x}^{(0)}) \cdot \mathbf{h}^{(0)} \pmod{p}. \tag{3}$$

Обозначим через $\theta_i = (\delta_{i,1}, \ldots, \delta_{i,n}) \in \mathcal{B}^n$, $i \in \{1, \ldots, n\}$, вектор, i-я компонента которого равна 1, а остальные равны 0 ($\delta_{i,j}$ — символ Кронекера). Используем сравнение (3) при $\mathbf{h} = \theta_i$:

$$\gamma_j f(\mathbf{x} + p^j \theta_i) \equiv \gamma_j f(x) + \frac{\partial f}{\partial x_i}(\mathbf{x}^{(0)}) \pmod{p}.$$

Отсюда

$$\frac{\partial f}{\partial x_i}(\mathbf{x}^{(0)}) \equiv \gamma_j f(\mathbf{x} + p^j \theta_i) - \gamma_j f(x) \pmod{p}.$$

Следовательно, если $\mathbf{x} = \mathbf{x}^{(0)}$, то

$$\frac{\partial f}{\partial x_i}(\mathbf{x}^{(0)}) \equiv \gamma_j f(\mathbf{x}^{(0)} + p^j \theta_i) - \gamma_j f(\mathbf{x}^{(0)}) \pmod{p}. \tag{4}$$

Как видно, в полученном сравнении левая часть не зависит от j и оно выполняется при всех $j \in \{1, \ldots, m-1\}$. Это доказывает следующее важное утверждение.

Утверждение 1. Для любой полиномиальной функции $f(\mathbf{x}) \in \mathcal{P}_{p^m}(n)$ и любого $i \in \{1, \ldots, n\}$ значение формальной частной производной $\dfrac{\partial g}{\partial x_i}(\mathbf{x}^{(0)}) \pmod{p}$ не зависит от представляющего $f(\mathbf{x})$ многочлена $g(\mathbf{x}) \in \mathbb{Z}_{p^m}[x_1, \ldots, x_n]$ и для любого $j \in \{1, \ldots, m-1\}$ верно сравнение (4).

Теперь, если подставить сравнение (4) в (3), получим

$$\gamma_j f(\mathbf{x} + p^j \mathbf{h}) \equiv \gamma_j f(\mathbf{x}) + \sum_{i=1}^{n} \left(\gamma_j f(\mathbf{x}^{(0)} + p^j \theta_i) - \gamma_j f(\mathbf{x}^{(0)})\right) h_i^{(0)} \pmod{p}.$$

Таким образом, переходя к равенству в поле $\mathcal{B}$, докажем следующую теорему.

Теорема 3. Для любой полиномиальной функции $f(\mathbf{x}) \in \mathcal{P}_{p^m}(n)$ и любых $j \in \{1, \ldots, m-1\}$, $\mathbf{h} = (h_1, \ldots, h_n) \in \mathbb{Z}_{p^m}^n$ справедливо равенство

$$\gamma_j f(\mathbf{x} + p^j \mathbf{h}) = \gamma_j f(\mathbf{x}) \oplus \sum_{i=1}^{n} \left(\gamma_j f(\mathbf{x}^{(0)} + p^j \theta_i) \ominus \gamma_j f(\mathbf{x}^{(0)})\right) \otimes h_i^{(0)},$$

где $\theta_i = (\delta_{i,1}, \ldots, \delta_{i,n})$, $i \in \{1, \ldots, n\}$; $\ominus$ — операция взятия противоположного элемента в аддитивной группе поля $\mathcal{B}$.

Из теоремы 3 вытекает, что для любой полиномиальной функции $f(\mathbf{x})$ значение $\gamma_j f(\mathbf{x} + p^j \mathbf{h})$, $\mathbf{h} = (h_1, \ldots, h_n) \in \mathbb{Z}_{p^m}^n$, можно вычислить, зная значения $\gamma_j f(\mathbf{x})$ и $\gamma_j f(\mathbf{x}^{(0)} + p^j \theta_i) \ominus \gamma_j f(\mathbf{x}^{(0)})$, $i = 1, \ldots, n$. Это приводит к следующему утверждению.

Утверждение 2. Если функция $f(\mathbf{x}) \in \mathcal{P}_{p^m}(n)$, то её j-я координатная функция $\gamma_j f(\mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(j)}) : \mathcal{B}^{nj} \to \mathcal{B}$, $j \in \{1, \ldots, m-1\}$, однозначно определяется по значениям на множестве $\{0, \ldots, p^j - 1\}^n$ и значениям $\gamma_j f(\theta + p^j \theta_i)$, $\theta \in \mathcal{B}^n$, $\theta_i = (\delta_{i,1}, \ldots, \delta_{i,n})$, $i \in \{1, \ldots, n\}$.

Доказательство. Пусть $\alpha = (a_1, \ldots, a_n) \in \mathbb{Z}_{p^m}^n$. Покажем, как, зная указанные в условии величины, вычислить $\gamma_j f(\alpha)$. Разделим каждое a_k на p^j, $k = 1, \ldots, n$, с остатком и представим вектор α в виде

$$\alpha = \beta + p^j \nu,$$

где $\beta = (b_1, \ldots, b_n) \in \{0, \ldots, p^j - 1\}^n$; $\nu = (v_1, \ldots, v_n) \in \mathbb{Z}_{p^m}^n$. Аналогично разделим каждое полученное v_k на p, $k = 1, \ldots, n$, с остатком и представим ν в виде

$$\nu = \theta + p\nu_1,$$

где $\theta = (h_1, \ldots, h_n) \in \mathcal{B}^n$; $\nu_1 \in \mathbb{Z}_{p^m}^n$.

Имеем

$$\alpha = \beta + p^j \nu = \beta + p^j(\theta + p\nu_1) = \beta + p^j\theta + p^{j+1}\nu_1.$$

В силу теоремы 1

$$\gamma_j f(\alpha) = \gamma_j f(\beta + p^j\theta + p^{j+1}\nu_1) = \gamma_j f(\beta + p^j\theta).$$

Тогда по теореме 3

$$\gamma_j f(\alpha) = \gamma_j f(\beta + p^j\theta) = \gamma_j f(\beta) \oplus \sum_{i=1}^{n} \big(\gamma_j f(\beta^{(0)} + p^j\theta_i) \ominus \gamma_j f(\beta^{(0)})\big) \otimes h_i^{(0)}.$$

При этом по условию утверждения известны значения $\gamma_j f(\beta)$, $\gamma_j f(\beta^{(0)})$ и $\gamma_j f(\beta^{(0)} + {}$ ${} + p^j\theta_i)$, а значит, используя полученное равенство, находим $\gamma_j f(\alpha)$. ■

Сформулируем утверждение о мощности класса полиномиальных функций над кольцом вычетов $\mathbb{Z}_{p^2}$. Его доказательство нетрудно получить, используя работу [6].

Утверждение 3. Для любого $n \in \mathbb{N}$ справедливо равенство

$$|\mathcal{P}_{p^2}(n)| = p^{p^n(n+2)}.$$

2. Класс ВКП-функций над кольцом вычетов

Введём понятие функций с вариационно-координатной полиномиальностью над кольцом вычетов, а также опишем некоторые их общие свойства. Дадим оценку мощности класса ВКП-функций над примарным кольцом вычетов и докажем утверждения о его соотношении с классом полиномиальных функций.

2.1. Определение класса ВКП-функций и его простейшие свойства

Определение 5. Функцию $f(\mathbf{x}) \in \mathcal{F}_{p^m}(n)$ назовём *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

$$\gamma_j f(\mathbf{x}) = \gamma_j p_j(\mathbf{x}),\ j = 0, \ldots, m-1. \qquad (5)$$

В таком случае будем говорить, что $p_j(\mathbf{x})$ является *многочленом j-й координаты функции $f(\mathbf{x})$* или её *j-м координатным многочленом.*

При этом в условиях определения 5 будем говорить, что функция $f(\mathbf{x})$ обладает свойством вариационно-координатной полиномиальности. Класс всех ВКП-функций от n переменных над $\mathbb{Z}_{p^m}$ обозначим через $\mathcal{CP}_{p^m}(n)$.

Поясним введённое определение. Произвольная функция $f(\mathbf{x}) \in \mathcal{F}_{p^m}(n)$ является вариационно-координатно-полиномиальной, если существуют такие многочлены, или полиномиальные функции $p_0(\mathbf{x}), p_1(\mathbf{x}), \ldots, p_{m-1}(\mathbf{x})$ над кольцом $\mathbb{Z}_{p^m}$, что выполнено равенство

$$f(\alpha) = \sum_{j=0}^{m-1} p^j \gamma_j p_j(\alpha) \tag{6}$$

для всех $\alpha \in \mathbb{Z}_{p^m}^n$. Использование при этом термина «вариационно» подчёркивает тот факт, что данные координатные многочлены могут быть разными для различных координат, т. е. могут меняться от координаты к координате. Если же все координатные многочлены одинаковы, то такая функция полиномиальна, поэтому справедливо включение

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

Следующая теорема устанавливает, что ВКП-функции, так же, как и полиномиальные функции, сохраняют отношение сравнимости по любому делителю p^m.

Теорема 4. При любом $n \in \mathbb{N}$ все ВКП-функции $f(\mathbf{x}) \in \mathcal{CP}_{p^m}(n)$ сохраняют отношение сравнимости по любому делителю p^m, т. е. справедливо включение

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

Доказательство. Если $f(\mathbf{x}) \in \mathcal{CP}_{p^m}(n)$, то существуют полиномиальные функции $p_0(\mathbf{x}), p_1(\mathbf{x}), \ldots, p_{m-1}(\mathbf{x})$, что выполнено равенство (6). В соответствии с теоремой 1 справедливо

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

а значит, $\gamma_j f(\mathbf{x}) = \gamma_j f(\mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(j)})$ и $f(\mathbf{x})$ является треугольной функцией, поэтому по теореме 1 $f(\mathbf{x}) \in \mathcal{D}_{p^m}(n)$. ■

Следствие 3. Для любой $f(\mathbf{x}) \in \mathcal{CP}_{p^m}(n)$ справедливо сравнение

$$\gamma_0 f(\mathbf{x}) \equiv p_0(\mathbf{x}^{(0)}) \pmod{p}. \tag{7}$$

Используя (7), можно в некотором смысле считать, что многочлен нулевой координаты ВКП-функции является многочленом над полем $\mathcal{B}$ и при этом задаёт функцию от младших координат аргументов:

$$\gamma_0 p_0(\mathbf{x}^{(0)})\colon \mathcal{B}^n \to \mathcal{B}.$$

Как известно, любая функция над полем $\mathcal{B}$ полиномиальна и при этом однозначно представима многочленом, у которого степени входящих в него переменных изменяются от 0 до $p-1$ [4]. Поэтому можно считать, что многочлен нулевой координаты определяется однозначно. Более того, по значениям самой функции $f(\mathbf{x}) \in \mathcal{CP}_{p^m}(n)$ его легко восстановить из сравнений $f(\alpha) \equiv p_0(a_1^{(0)}, \ldots, a_n^{(0)}) \pmod{p}$, $\alpha \in \mathbb{Z}_{p^m}^n$.

Следующая теорема говорит о строении координатных функций $\gamma_j f$ ВКП-функций, рассматриваемых над полем $\mathcal{B}$; при этом, как и ранее, будем предполагать, что порядок следования их переменных идёт с возрастанием номеров координат.

Теорема 5 (о строении координатных функций). Если $f(\mathbf{x}) \in \mathcal{CP}_{p^m}(n)$, то для любого $j \in \{1, \ldots, m-1\}$ существуют полиномиальные 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 выполнено равенство

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

Доказательство. Действительно, согласно равенству (3),

$$\gamma_j f(\mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(j)}) = \gamma_j p_j(\mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(j)}) = \gamma_j p_j(\mathbf{x}^{(0)} + \ldots + p^{j-1}\mathbf{x}^{(j-1)} + p^j \mathbf{x}^{(j)}) \equiv$$
$$\equiv \gamma_j p_j(\mathbf{x}^{(0)} + \ldots + p^{j-1}\mathbf{x}^{(j-1)}) + \operatorname{grad} p_j(\mathbf{x}^{(0)}) \cdot \mathbf{x}^{(j)} \pmod p.$$

Функция $\gamma_j p_j(\mathbf{x}^{(0)} + \ldots + p^{j-1}\mathbf{x}^{(j-1)}) \colon \mathcal{B}^{jn} \to \mathcal{B}$, рассматриваемая как функция над полем $\mathcal{B}$, представима над ним некоторым многочленом g_j от переменных $\mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(j-1)}$. Аналогично, существуют полиномиальные функции $g_{ji}(\mathbf{x}^{(0)}) \colon \mathcal{B}^n \to \mathcal{B}$, $i = 1, \ldots, n$, над полем $\mathcal{B}$, такие, что $\dfrac{\partial p_j}{\partial x_i}(\mathbf{x}^{(0)}) \equiv g_{ji}(\mathbf{x}^{(0)}) \pmod p$. Отсюда имеем сравнение

$$\operatorname{grad} p_j(\mathbf{x}^{(0)}) \cdot \mathbf{x}^{(j)} = \sum_{i=1}^{n} \frac{\partial p_j}{\partial x_i}(\mathbf{x}^{(0)}) x_i^{(j)} \equiv \sum_{i=1}^{n} g_{ji}(\mathbf{x}^{(0)}) \otimes x_i^{(j)} \pmod p,$$

которое, при переходе к равенству в поле $\mathcal{B}$, завершает доказательство теоремы. ■

В частном случае, когда функция $f(\mathbf{x})$ полиномиальна, для функций g_{ji} справедливо сравнение

$$\frac{\partial f}{\partial x_i}(\mathbf{x}^{(0)}) \equiv g_{ji}(\mathbf{x}^{(0)}) \pmod p,$$

из которого следует, что g_{ji} не зависят от j. Это доказывает

Следствие 4. Если $f(\mathbf{x}) \in \mathcal{P}_{p^m}(n)$, то существуют полиномиальные функции $g_i \colon \mathcal{B}^n \to \mathcal{B}$, $i = 1, \ldots, n$, над полем $\mathcal{B}$ и для любого $j \in \{1, \ldots, m-1\}$ существуют полиномиальные функции $g_j \colon \mathcal{B}^{jn} \to \mathcal{B}$ над полем $\mathcal{B}$, такие, что выполнено равенство

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

Пример 1. Рассмотрим ВКП-функцию $f(x)$ (см. таблицу) над $\mathbb{Z}_8$ с координатными многочленами $p_0(x) = x$, $p_1(x) = 3x^3 + 2$, $p_2(x) = 5x^3 + x + 7$. Её координатные функции над полем $\mathcal{B} = \{0, 1\}$ имеют вид

$$\gamma_0 f(x) = x^{(0)},\ \gamma_1 f(x) = x^{(0)} \otimes x^{(1)} \oplus x^{(0)} \oplus 1,\ \gamma_2 f(x) = (x^{(0)} \oplus 1) \otimes x^{(2)} \oplus x^{(1)} \oplus 1.$$

x	0	1	2	3	4	5	6	7
$f(x)$	6	5	2	3	2	5	6	3

Теорема 5 свидетельствует о свойстве ВКП-функций, играющем важную роль при решении систем уравнений

$$\begin{cases} f_1(x_1, \ldots, x_n) = y_1, \\ \quad\vdots \\ f_l(x_1, \ldots, x_n) = y_l, \end{cases}$$

где $y_i \in \mathbb{Z}_{p^m}$; $f_i \in \mathcal{CP}_{p^m}(n)$, $i = 1, \ldots, l$ (в дальнейшем такие системы будем называть системами ВКП-уравнений). Идея использования данного свойства заключается в следующем. При нахождении координат неизвестных переменных до j-го порядка включительно $(j+1)$-я координатная функция каждой из ВКП-функций, входящих в систему, становится аффинной относительно неизвестных $(j+1)$-х координат, а значит, можно свести задачу их нахождения к решению некоторой системы линейных уравнений над полем $\mathcal{B}$.

Сформулируем и докажем формулу Тейлора для ВКП-функций, обобщающую формулу (1). Этот результат в определённом смысле оправдывает терминологию «полиномиальность» в названии ВКП-функций.

Теорема 6 (формула Тейлора). Если функция $f(\mathbf{x}) \in \mathcal{CP}_{p^m}(n)$ и $p_0(\mathbf{x}), \ldots, p_{m-1}(\mathbf{x})$ — её координатные многочлены, то для любых $j \in \{1, \ldots, m-1\}$ и $\mathbf{h} \in \mathbb{Z}_{p^m}^n$ справедливо сравнение

$$f(\mathbf{x} + p^j\mathbf{h}) \equiv f(\mathbf{x}) + p^j \operatorname{grad} p_j(\mathbf{x}) \cdot \mathbf{h} \pmod{p^{j+1}}. \tag{8}$$

Доказательство. В соответствии с формулой (3) имеем сравнение

$$\gamma_j f(\mathbf{x} + p^j\mathbf{h}) = \gamma_j p_j(\mathbf{x} + p^j\mathbf{h}) \equiv \gamma_j p_j(\mathbf{x}) + \operatorname{grad} p_j(\mathbf{x}^{(0)}) \cdot \mathbf{h}^{(0)} \pmod{p}.$$

В силу сравнимости $\operatorname{grad} p_j(\mathbf{x}^{(0)}) \cdot \mathbf{h}^{(0)} \equiv \operatorname{grad} p_j(\mathbf{x}) \cdot \mathbf{h} \pmod{p}$ запишем

$$\gamma_j p_j(\mathbf{x} + p^j\mathbf{h}) \equiv \gamma_j p_j(\mathbf{x}) + \operatorname{grad} p_j(\mathbf{x}) \cdot \mathbf{h} \pmod{p}. \tag{9}$$

Теперь воспользуемся равенством (6) и приведём его по модулю p^{j+1}, в результате получим сравнение

$$f(\mathbf{x} + p^j\mathbf{h}) \equiv \sum_{i=0}^{j} p^i \gamma_i p_i(\mathbf{x} + p^j\mathbf{h}) \pmod{p^{j+1}}. \tag{10}$$

Так как $p_i(\mathbf{x}) \in \mathcal{D}_{p^m}(n)$, $i = 0, \ldots, j-1$, то из свойств функций, сохраняющих отношение сравнимости, очевидно, следует равенство $\gamma_i p_i(\mathbf{x} + p^j\mathbf{h}) = \gamma_i p_i(\mathbf{x})$. Подставив данные равенства и сравнение (9) в (10), получим

$$f(\mathbf{x} + p^j\mathbf{h}) \equiv \sum_{i=0}^{j-1} p^i \gamma_i p_i(\mathbf{x}) + p^j(\gamma_j p_j(\mathbf{x}) + \operatorname{grad} p_j(\mathbf{x}) \cdot \mathbf{h} \pmod{p^{j+1}}.$$

Отсюда $f(\mathbf{x} + p^j\mathbf{h}) \equiv \sum_{i=0}^{j} p^i \gamma_i p_i(\mathbf{x}) + p^j \operatorname{grad} p_j(\mathbf{x}) \cdot \mathbf{h} \pmod{p^{j+1}}$. Осталось заметить, что $\sum_{i=0}^{j} p^i \gamma_i p_i(\mathbf{x}) \equiv f(\mathbf{x}) \pmod{p^{j+1}}$ и, следовательно, справедливо сравнение (8). ∎

Следствие 5. Если функция $f(\mathbf{x}) \in \mathcal{CP}_{p^m}(n)$ и $p_0(\mathbf{x}), \ldots, p_{m-1}(\mathbf{x})$ — её координатные многочлены, то для любых $j \in \{1, \ldots, m-1\}$ и $\mathbf{h} \in \mathbb{Z}_{p^m}^n$ справедливо сравнение

$$f(\mathbf{x} + p^j\mathbf{h}) \equiv f(\mathbf{x}) + p^j \operatorname{grad} p_j(\mathbf{x}^{(0)}) \cdot \mathbf{h}^{(0)} \pmod{p^{j+1}}. \tag{11}$$

В заключение данного подраздела дадим определение ВКП-функции над произвольным кольцом вычетов $\mathbb{Z}_k$, $k \in \mathbb{N}$, $k > 1$. При этом при $m = 1$ положим по определению, что над полем вычетов по модулю p класс ВКП-функций равен классу полиномиальных (или, что то же самое, совпадает с классом всех функций $\mathcal{F}_p(n)$). Другими словами,

$$\mathcal{CP}_p(n) = \mathcal{P}_p(n).$$

Определение 6. Функцию $f(\mathbf{x}) \in \mathcal{F}_k(n)$ будем называть *ВКП-функцией* над кольцом вычетов $\mathbb{Z}_k$, где $k = p_1^{m_1} \cdot \ldots \cdot p_t^{m_t}$ — каноническое разложение числа k, если одновременно выполняются следующие два условия:

— $f(\mathbf{x})$ сохраняет отношение сравнимости по модулю $p_i^{m_i}$, $i = 1, \ldots, t$;

— $f_i(\mathbf{x}) \in \mathcal{F}_{p_i^{m_i}}(n)$, где $f_i(\mathbf{x}) \equiv f(\mathbf{x}) \pmod{p_i^{m_i}}$, является ВКП-функцией над примарным кольцом вычетов $\mathbb{Z}_{p_i^{m_i}}$, $i = 1, \ldots, t$.

В частности, как легко видеть, непосредственно из данного определения следует, что класс полиномиальных над $\mathbb{Z}_k$ функций содержится в классе ВКП-функций над этим кольцом. Класс всех ВКП-функций от n переменных над кольцом вычетов $\mathbb{Z}_k$ обозначим через $\mathcal{CP}_k(n)$.

2.2. Оценка числа ВКП-функций от n переменных над $\mathbb{Z}_{p^m}$

Поскольку каждая ВКП-функция однозначно определяется соответствующими координатными отображениями полиномиальных функций, то их количество равно произведению мощностей классов таких отображений. При $j = 0$ количество различных координатных отображений $\gamma_0 p(\mathbf{x})$ (где $p(\mathbf{x}) \in \mathcal{P}_{p^m}(n)$) определяется числом всех функций от n переменных над полем $\mathcal{B}$ (см. формулу (7)) и равно p^{p^n}. Для каждого $j \in \{1, \ldots, m-1\}$ оценим сверху количество различных $\gamma_j p(\mathbf{x})$ (где $p(\mathbf{x}) \in \mathcal{P}_{p^m}(n)$), что даст верхнюю оценку мощности класса $\mathcal{CP}_{p^m}(n)$.

Утверждение 4. Для любого $n \in \mathbb{N}$ верна оценка числа ВКП-функций от n переменных над $\mathbb{Z}_{p^m}$:

$$\log_p |\mathcal{CP}_{p^m}(n)| \leqslant p^n + (m-1)np^n + \frac{p^n(p^{n(m-1)} - 1)}{p^n - 1}. \qquad (12)$$

Доказательство. Согласно утверждению 2, j-е координатное отображение, $j \in \{1, \ldots, m-1\}$, любой полиномиальной функции однозначно определяется по значениям на множестве $\{0, \ldots, p^j - 1\}^n$ и векторах вида $\theta + p^j\theta_i$, $\theta \in \mathcal{B}^n$, $\theta_i = (\delta_{i,1}, \ldots, \delta_{i,n})$, $i \in \{1, \ldots, n\}$. Количество таких значений равно в точности $p^{jn} + np^n$. А значит, число всех различных j-х координатных отображений полиномиальных функций от n переменных над $\mathbb{Z}_{p^m}$ не превосходит $p^{p^{jn} + n \cdot p^n}$. Отсюда получим оценку мощности класса $\mathcal{CP}_{p^m}(n)$:

$$|\mathcal{CP}_{p^m}(n)| \leqslant p^{p^n} \prod_{j=1}^{m-1} p^{p^{jn} + np^n} = p^{p^n} p^{\sum\limits_{j=1}^{m-1}(p^{jn} + np^n)} = p^{p^n + (m-1)np^n + \dfrac{p^n(p^{n(m-1)} - 1)}{p^n - 1}}.$$

Утверждение доказано. ■

2.3. Соотношение между классами полиномиальных и ВКП-функций

Ранее было отмечено, что класс полиномиальных функций над кольцом вычетов вкладывается в класс ВКП-функций. Ответим на вопрос о строгости этого вложения. Сначала рассмотрим случай примарных колец вычетов.

Теорема 7. Для любого $n \in \mathbb{N}$ классы полиномиальных и ВКП-функций над $\mathbb{Z}_{p^2}$ от n переменных совпадают, т. е.

$$\mathcal{P}_{p^2}(n) = \mathcal{CP}_{p^2}(n).$$

Доказательство. Согласно утверждению 3,

$$|\mathcal{P}_{p^2}(n)| = p^{p^n(n+2)}.$$

С другой стороны, согласно неравенству (12),

$$|\mathcal{CP}_{p^2}(n)| \leqslant p^{p^n+np^n+p^n} = p^{p^n(n+2)}.$$

А значит, $|\mathcal{CP}_{p^2}(n)| \leqslant |\mathcal{P}_{p^2}(n)|$. Но при этом $\mathcal{P}_{p^2}(n) \subseteq \mathcal{CP}_{p^2}(n)$. Следовательно, имеет место равенство $\mathcal{P}_{p^2}(n) = \mathcal{CP}_{p^2}(n)$. ■

Следствие 6. Если $k = p_1^{m_1} \cdot \ldots \cdot p_t^{m_t}$ — каноническое разложение числа $k \in \mathbb{N}$, $k > 1$, и $m_i \in \{1, 2\}$, $i = 1, \ldots, t$, то для любого $n \in \mathbb{N}$ справедливо равенство

$$\mathcal{P}_k(n) = \mathcal{CP}_k(n).$$

Доказательство. Если $f(\mathbf{x}) \in \mathcal{CP}_k(n)$, то функция $f_i(\mathbf{x}) \equiv f(\mathbf{x}) \pmod{p_i^{m_i}}$, $f_i \in \mathcal{F}_{p_i^{m_i}}(n)$, $i = 1, \ldots, t$, в силу теоремы 7 при $m_i = 2$ и равенства $\mathcal{CP}_p(n) = \mathcal{P}_p(n)$, полиномиальна. А значит, и $f(\mathbf{x})$ полиномиальна. ■

Чтобы показать, что при $m \geqslant 3$ существуют не полиномиальные ВКП-функции над $\mathbb{Z}_{p^m}$, докажем следующую теорему о достаточном условии отсутствия полиномиального представления для функции из данного класса.

Теорема 8. Пусть функция $f(\mathbf{x}) \in \mathcal{CP}_{p^m}(n)$, $m \geqslant 3$, и $p_0(\mathbf{x}), \ldots, p_{m-1}(\mathbf{x})$ — её координатные многочлены. Если существуют $i, j \in \{1, \ldots, m-1\}$, $i \neq j$, и $\alpha \in \mathcal{B}^n$, такие, что

$$\operatorname{grad} p_i(\alpha) \not\equiv \operatorname{grad} p_j(\alpha) \pmod{p},$$

то $f(\mathbf{x}) \notin \mathcal{P}_{p^m}(n)$.

Доказательство. Так как $\operatorname{grad} p_i(\alpha) \not\equiv \operatorname{grad} p_j(\alpha) \pmod{p}$, то существует $s \in \{1, \ldots, n\}$, такое, что

$$\frac{\partial p_i}{\partial x_s}(\alpha) \not\equiv \frac{\partial p_j}{\partial x_s}(\alpha) \pmod{p}. \tag{13}$$

Предположим, что функция $f(\mathbf{x})$ полиномиальна и представима некоторым многочленом $g(\mathbf{x}) \in \mathbb{Z}_{p^m}[x_1, \ldots, x_n]$. Тогда в соответствии с утверждением 1 (сравнение (4)) справедливо сравнение

$$\frac{\partial g}{\partial x_s}(\alpha) \equiv \gamma_k f(\alpha + p^k\theta_s) - \gamma_k f(\alpha) \pmod{p},\ k = 1, \ldots, m-1.$$

В частности, при $k = i$ имеем

$$\frac{\partial g}{\partial x_s}(\alpha) \equiv \gamma_i f(\alpha + p^i\theta_s) - \gamma_i f(\alpha) = \gamma_i p_i(\alpha + p^i\theta_s) - \gamma_i p_i(\alpha) \equiv \frac{\partial p_i}{\partial x_s}(\alpha) \pmod{p}.$$

Таким образом, справедливо сравнение $\frac{\partial g}{\partial x_s}(\alpha) \equiv \frac{\partial p_i}{\partial x_s}(\alpha) \pmod{p}$. Применяя те же рассуждения при $k = j$, получим

$$\frac{\partial g}{\partial x_s}(\alpha) \equiv \frac{\partial p_i}{\partial x_s}(\alpha) \equiv \frac{\partial p_j}{\partial x_s}(\alpha) \pmod{p},$$

что противоречит (13), а значит, и полиномиальности функции $f(\mathbf{x})$. ■

Пример 2. Вернемся к рассмотрению ВКП-функции $f(x)$ над $\mathbb{Z}_8$ из примера 1. Найдём формальные производные многочленов $p_1(x)$ и $p_2(x)$:

$$p_1'(x) = x^2 \equiv x \pmod 2, \quad p_2'(x) = 7x^2 + 1 \equiv x + 1 \pmod 2.$$

Ясно, что при любом $\alpha \in \mathcal{B} = \{0,1\}$ $p_1'(\alpha) \not\equiv p_2'(\alpha) \pmod 2$, поэтому выполнено условие теоремы 8, а значит, $f(x)$ не является полиномиальной.

Используя теорему 8, можно доказать утверждение о соотношении классов полиномиальных и ВКП-функций над $\mathbb{Z}_{p^m}$ при $m \geqslant 3$.

Утверждение 5. Для любых $n \in \mathbb{N}$ и $m \geqslant 3$ класс ВКП-функций $\mathcal{CP}_{p^m}(n)$ не совпадает с классом полиномиальных $\mathcal{P}_{p^m}(n)$.

Доказательство. Действительно, достаточно рассмотреть ВКП-функцию $f(\mathbf{x}) \in \mathcal{CP}_{p^m}(n)$, у которой координатные многочлены $p_1(\mathbf{x}) = x_1$, $p_2(\mathbf{x}) = 0$, а остальные многочлены произвольны. Тогда ясно, что при любом $\alpha \in \mathcal{B}^n$

$$\operatorname{grad} p_1(\alpha) = (1, 0, \ldots, 0) \not\equiv \operatorname{grad} p_2(\alpha) = (0, \ldots, 0).$$

Поэтому $f(\mathbf{x}) \notin \mathcal{P}_{p^m}(n)$. ■

Следствие 7. Если $k = p_1^{m_1} \cdot \ldots \cdot p_t^{m_t}$ — каноническое разложение числа $k \in \mathbb{N}$, $k > 1$, и $m_j \geqslant 3$ для некоторого $j \in \{1, \ldots, t\}$, то для любого $n \in \mathbb{N}$ справедливо строгое включение

$$\mathcal{P}_k(n) \subsetneq \mathcal{CP}_k(n).$$

Доказательство. Рассмотрим произвольные ВКП-функции $f_i(\mathbf{x}) \in \mathcal{CP}_{p_i^{m_i}}(n)$, $i = 1, \ldots, t$, при этом, так как $m_j \geqslant 3$, можно выбрать ВКП-функцию $f_j(\mathbf{x}) \notin \mathcal{P}_{p_j^{m_j}}(n)$.

Построим ВКП-функцию $f(\mathbf{x})$ над $\mathbb{Z}_k$ следующим образом. Для любого $\alpha \in \mathbb{Z}_k^n$ если выполнена система сравнений

$$\begin{cases} \alpha \equiv \alpha_1 \pmod{p_1^{m_1}}, \\ \qquad\vdots \\ \alpha \equiv \alpha_t \pmod{p_t^{m_t}}, \end{cases}$$

где $\alpha_i \in \mathbb{Z}^n_{p_i^{m_i}}$, $i = 1, \ldots, t$, то положим значение $f(\alpha) \in \mathbb{Z}_k$ таким, чтобы была выполнена система сравнений

$$\begin{cases} f(\alpha) \equiv f_1(\alpha_1) \pmod{p_1^{m_1}}, \\ \qquad\vdots \\ f(\alpha) \equiv f_t(\alpha_t) \pmod{p_t^{m_t}}. \end{cases}$$

Легко проверить, что определённая таким образом функция $f(\mathbf{x})$ сохраняет отношение сравнимости по модулю $p_i^{m_i}$, $i = 1, \ldots, t$, и $f(\mathrm{x}) \equiv f_i(\mathbf{x}) \pmod p_i^{m_i}$, $i = 1, \ldots, t$. Следовательно, $f(\mathbf{x})$ является ВКП-функцией и при этом $f(\mathbf{x}) \notin \mathcal{P}_k(n)$ (иначе получим противоречие с тем, что $f_j(\mathbf{x}) \notin \mathcal{P}_{p_j^{m_j}}(n)$). ■

3. Метод покоординатной линеаризации для решения систем ВКП-уравнений

Опишем алгоритм решения систем ВКП-уравнений над примарным кольцом вычетов, являющийся обобщением метода покоординатной линеаризации для решения систем полиномиальных уравнений (см. также [7]). Будем при этом предполагать, что для каждой ВКП-функции $f_i(\mathbf{x})$, $i = 1, \ldots, l$, из системы уравнений

$$\begin{cases} f_1(\mathbf{x}) = y_1, \\ \quad\vdots \\ f_l(\mathbf{x}) = y_l, \end{cases} \tag{14}$$

где $y_i \in \mathbb{Z}_{p^m}$; $f_i \in \mathcal{CP}_{p^m}(n)$, $i = 1, \ldots, l$, известны её координатные многочлены $p_{ij}(\mathbf{x})$, $j = 0, \ldots, m-1$.

1. Приведём систему (14) по модулю p. В силу сравнения (7) получим систему полиномиальных уравнений над полем $(\mathcal{B}, \oplus, \otimes)$ относительно младших координат неизвестных переменных:

$$\begin{cases} \gamma_0 f_1(\mathbf{x}^{(0)}) \equiv y_1^{(0)}, \\ \quad\vdots \\ \gamma_0 f_l(\mathbf{x}^{(0)}) \equiv y_l^{(0)} \end{cases} \pmod p \;\Leftrightarrow \begin{cases} p_{10}(\mathbf{x}^{(0)}) \equiv y_1^{(0)}, \\ \quad\vdots \\ p_{l0}(\mathbf{x}^{(0)}) \equiv y_l^{(0)} \end{cases} \pmod p. \tag{15}$$

Полученную систему необходимо решить каким-либо образом и найти все возможные значения $\mathbf{c}^{(0)} = (c_1^{(0)}, \ldots, c_n^{(0)}) \in \mathcal{B}^n$ координат $\mathbf{x}^{(0)}$. Если система несовместна, то алгоритм заканчивает работу и исходная система (14) не имеет решений.

2. Пусть при $j \in \{1, \ldots, m\}$ найдены все значения $\mathbf{c}^{(0)}$, …, $\mathbf{c}^{(j-1)}$ координат $\mathbf{x}^{(0)}$, …,$\mathbf{x}^{(j-1)}$ соответственно, которые в силу того, что f_i являются треугольными функциями, т. е. $f_i \in \mathcal{D}_{p^m}(n)$, $i = 1, \ldots, l$, удовлетворяют системам сравнений вида

$$\begin{cases} f_1(\mathbf{x}) \equiv y_1, \\ \quad\vdots \\ f_l(\mathbf{x}) \equiv y_l \end{cases} \pmod{p^j} \;\Leftrightarrow \begin{cases} f_1(\mathbf{c}^{(0)}, \ldots, \mathbf{c}^{(j-1)}) \equiv y_1, \\ \quad\vdots \\ f_l(\mathbf{c}^{(0)}, \ldots, \mathbf{c}^{(j-1)}) \equiv y_l \end{cases} \pmod{p^j}. \tag{16}$$

Если $j = m$, то перейти к п. 3. Иначе при любом таком наборе координат неизвестных $\mathbf{c}^{(0)}, \ldots, \mathbf{c}^{(j-1)}$ выполним следующие действия. Приведём систему (14) по модулю p^{j+1}, в результате получим систему сравнений вида

$$\begin{cases} f_1(\mathbf{c}^{(0)}, \ldots, \mathbf{c}^{(j-1)}, \mathbf{x}^{(j)}) \equiv y_1, \\ \quad\vdots \\ f_l(\mathbf{c}^{(0)}, \ldots, \mathbf{c}^{(j-1)}, \mathbf{x}^{(j)}) \equiv y_l \end{cases} \pmod{p^{j+1}}. \tag{17}$$

Рассмотрим i-е уравнение полученной системы, $i \in \{1, \ldots, l\}$:

$$f_i(\mathbf{c}^{(0)}, \ldots, \mathbf{c}^{(j-1)}, \mathbf{x}^{(j)}) \equiv y_i \pmod{p^{j+1}}.$$

Воспользуемся сравнением (11):

$$f_i(\mathbf{c}^{(0)}, \ldots, \mathbf{c}^{(j-1)}, \mathbf{x}^{(j)}) = f_i(\mathbf{c}^{(0)} + \ldots + p^{j-1}\mathbf{c}^{(j-1)} + p^j \mathbf{x}^{(j)}) \equiv$$
$$\equiv f_i(\mathbf{c}^{(0)}, \ldots, \mathbf{c}^{(j-1)}) + p^j \operatorname{grad} p_{ij}(\mathbf{c}^{(0)}) \cdot \mathbf{x}^{(j)} \equiv y_i \pmod{p^{j+1}}.$$

В силу (16) справедливо сравнение $f_i(\mathbf{c}^{(0)}, \ldots, \mathbf{c}^{(j-1)}) \equiv y_i \pmod{p^j}$, а значит,

$$f_i(\mathbf{c}^{(0)}, \ldots, \mathbf{c}^{(j-1)}) \equiv y_i^{(0)} + \ldots + p^{j-1} y_i^{(j-1)} + p^j \gamma_j f_i(\mathbf{c}^{(0)}, \ldots, \mathbf{c}^{(j-1)}) \pmod{p^{j+1}}.$$

Отсюда имеем

$$y_i^{(0)}+\ldots+p^{j-1}y_i^{(j-1)}+p^j\gamma_j f_i(\mathbf{c}^{(0)},\ldots,\mathbf{c}^{(j-1)})+p^j\operatorname{grad}p_{ij}(\mathbf{c}^{(0)})\cdot\mathbf{x}^{(j)}\equiv y_i \pmod{p^{j+1}}.$$

Приходим к равенству в поле $\mathcal{B}$:

$$p^j\gamma_j f_i(\mathbf{c}^{(0)},\ldots,\mathbf{c}^{(j-1)})+p^j\operatorname{grad}p_{ij}(\mathbf{c}^{(0)})\cdot\mathbf{x}^{(j)}\equiv p^j y_i^{(j)} \pmod{p^{j+1}} \Leftrightarrow$$
$$\Leftrightarrow \operatorname{grad}p_{ij}(\mathbf{c}^{(0)})\otimes\mathbf{x}^{(j)}=_{\mathcal{B}} y_i^{(j)}\ominus\gamma_j f_i(\mathbf{c}^{(0)},\ldots,\mathbf{c}^{(j-1)}).$$

Применив таким образом указанные преобразования и рассуждения к каждому уравнению системы (17), получим равносильную ей систему линейных уравнений относительно неизвестных координат $\mathbf{x}^{(j)}$ над полем $\mathcal{B}$:

$$\begin{pmatrix}\operatorname{grad}p_{1j}(\mathbf{c}^{(0)})\\ \vdots\\ \operatorname{grad}p_{lj}(\mathbf{c}^{(0)})\end{pmatrix}\otimes\mathbf{x}^{(j)}=_{\mathcal{B}}\begin{pmatrix}y_1^{(j)}\ominus\gamma_j f_1(\mathbf{c}^{(0)},\ldots,\mathbf{c}^{(j-1)})\\ \vdots\\ y_l^{(j)}\ominus\gamma_j f_l(\mathbf{c}^{(0)},\ldots,\mathbf{c}^{(j-1)})\end{pmatrix}. \tag{18}$$

Матрица полученной системы линейных уравнений является матрицей Якоби $\mathcal{J}_{F_j}(\mathbf{c}^{(0)}) \pmod p$ (т. е. приведённой по модулю p) полиномиальной вектор-функции $F_j=(p_{1j},\ldots,p_{lj})$ в точке $\mathbf{c}^{(0)}\in\mathcal{B}^n$. Решая полученную линейную систему над $\mathcal{B}$, найдём все возможные значения координат $\mathbf{x}^{(j)}$ (при заданных координатах $\mathbf{x}^{(0)}=\mathbf{c}^{(0)}$, $\ldots$, $\mathbf{x}^{(j-1)}=\mathbf{c}^{(j-1)}$).

При всех $\mathbf{x}^{(0)},\ldots,\mathbf{x}^{(j-1)}$, удовлетворяющих системе (16), необходимо решить систему (18) и найти все возможные значения координат $\mathbf{x}^{(j)}$. Если таких $\mathbf{x}^{(j)}$ нет (т. е. система (18) несовместна при любых $\mathbf{x}^{(0)},\ldots,\mathbf{x}^{(j-1)}$, удовлетворяющих системе (16)), то исходная система (14) несовместна и алгоритм заканчивает работу. Увеличить j на 1 и перейти к п. 2 алгоритма.

3. Если найдены все координаты переменных $\mathbf{x}^{(0)}=\mathbf{c}^{(0)}$, $\ldots$, $\mathbf{x}^{(m-1)}=\mathbf{c}^{(m-1)}$, которые удовлетворяют системе (16) при $j=m$, то решения $\mathbf{c}=(c_1,\ldots,c_n)$ системы вычисляются следующим образом:

$$\mathbf{c}=\sum_{j=0}^{m-1}p^j\mathbf{c}^{(j)},$$

и на этом алгоритм завершает свою работу.

Теорема 9. Алгоритм решения системы ВКП-уравнений (14) находит все решения или доказывает её несовместность.

Доказательство. Вектор $\mathbf{c}=(c_1,\ldots,c_n)\in\mathbb{Z}_{p^m}^n$ является решением системы (14) тогда и только тогда, когда при любом $j\in\{0,\ldots,m-1\}$ координаты $\mathbf{c}^{(0)},\ldots,\mathbf{c}^{(j)}$ данного вектора удовлетворяют системе

$$\left\{\begin{array}{l} f_1(\mathbf{c}^{(0)},\ldots,\mathbf{c}^{(j)})\equiv y_1,\\ \quad\vdots\\ f_l(\mathbf{c}^{(0)},\ldots,\mathbf{c}^{(j)})\equiv y_l\end{array}\right. \pmod{p^{j+1}}.$$

Но, как видно, данный алгоритм последовательно при каждом $j\in\{0,\ldots,m-1\}$ находит все такие координаты $\mathbf{c}^{(0)},\ldots,\mathbf{c}^{(j)}$, которые удовлетворяют указанной системе. А значит, находит все решения исходной системы (14) либо доказывает её несовместность. ■

Приведём некоторые сложностные оценки описанного алгоритма.

Утверждение 6. Пусть $\{\mathbf{c}_1^{(0)}, \ldots, \mathbf{c}_t^{(0)}\}$ — все решения системы (15), $t \in \mathbb{N}$, $k_{ij} = \operatorname{rang} \mathcal{J}_{F_j}(\mathbf{c}_i^{(0)})$, $i = 1, \ldots, t$, $F_j = (p_{1j}, \ldots, p_{lj})$ и $l = \mathrm{O}(n)$. Тогда сложность S приведённого алгоритма оценивается сверху величиной

$$S \leqslant T_0 + \mathrm{O}\left(n^3 t \sum_{j=0}^{m-2} p^{j(n-k)}\right),$$

где T_0 — сложность решения системы (15); $k = \min\{k_1, \ldots, k_t\}$, $k_i = \min\{k_{i1}, \ldots, k_{i,m-1}\}$, $i = 1, \ldots, t$.

Доказательство. Пусть $\mathbf{c}_i^{(0)}$, $i \in \{1, \ldots, t\}$, — фиксированное решение системы (15). Если $k_{ij} = \operatorname{rang} \mathcal{J}_{F_j}(\mathbf{c}_i^{(0)})$, то в п. 2 алгоритма система (18) в случае совместности имеет $p^{n-k_{is}}$ решений для $\mathbf{x}^{(s)}$, $s = 1, \ldots, m-1$ (при фиксированных предыдущих значениях координат $\mathbf{c}^{(1)}, \ldots, \mathbf{c}^{(s-1)}$). Отсюда в «худшем» случае для нахождения $\mathbf{x}^{(1)}$ потребуется решить одну систему линейных уравнений над полем $\mathcal{B}$ со сложностью $\mathrm{O}(n^3)$, а для нахождения всех возможных значений координат $\mathbf{x}^{(j)}$, $j \in \{2, \ldots, m-1\}$, — решить $p^{n-k_{i1}} \cdot \ldots \cdot p^{n-k_{i,j-1}} = p^{n(j-1) - \sum_{s=1}^{j-1} k_{is}}$ систем линейных уравнений. Тогда сложность нахождения всех возможных значений $\mathbf{x}^{(j)}$, $j \in \{2, \ldots, m-1\}$ (при заданном $\mathbf{c}_i^{(0)}$, $i \in \{1, \ldots, t\}$) составит в «худшем» случае $S_j = \mathrm{O}\left(n^3 p^{n(j-1) - \sum_{s=1}^{j-1} k_{is}}\right)$. Если $k_i = \min\{k_{i1}, \ldots, k_{i,m-1}\}$, то при любом $j \in \{2, \ldots, m-1\}$ полученное S_j можно оценить следующим образом:

$$S_j \leqslant \mathrm{O}(n^3 p^{n(j-1) - \sum_{s=1}^{j-1} k_{is}}) \leqslant \mathrm{O}(n^3 p^{(j-1)(n-k_i)}).$$

При этом данная оценка справедлива и при $j = 1$. Отсюда сложность S решения системы (14) не превосходит величины

$$S = T_0 + \sum_{i=1}^{t} \sum_{j=1}^{m-1} S_j \leqslant T_0 + \sum_{i=1}^{t} \sum_{j=0}^{m-2} \mathrm{O}(n^3 p^{j(n-k_i)}) = T_0 + \mathrm{O}\left(n^3 \sum_{i=1}^{t} \sum_{j=0}^{m-2} p^{j(n-k_i)}\right) \leqslant$$
$$\leqslant T_0 + \mathrm{O}\left(n^3 \sum_{i=1}^{t} \sum_{j=0}^{m-2} p^{j(n-k)}\right) = T_0 + \mathrm{O}\left(n^3 t \sum_{j=0}^{m-2} p^{j(n-k)}\right).$$

Утверждение доказано. ■

Следствие 8. В условиях утверждения 6 справедливо:

1) если $k \neq n$, то сложность S алгоритма оценивается сверху величиной

$$S \leqslant T_0 + \mathrm{O}\left(n^3 t \frac{p^{(m-1)(n-k)} - 1}{p^{n-k} - 1}\right);$$

2) если $k = n$, то сложность алгоритма оценивается сверху величиной

$$S \leqslant T_0 + \mathrm{O}(n^3 t(m-1)).$$

Заметим, что если $k = n$ в условиях утверждения 6, то и все $k_{ij} = n$ для $i = 1, \ldots, t$, $j = 1, \ldots, m-1$, а значит, система (18) на каждом шаге $j \in \{1, \ldots, m-1\}$ (при любом фиксированном решении системы (15)) имеет не более одного решения. И в «худшем» случае алгоритм сводится к t-кратному решению $(m-1)$ системы линейных уравнений над полем $\mathcal{B}$.

Следствие 9. Если система (15) имеет единственное решение $\mathbf{c}^{(0)}$, $l = n$ и $\operatorname{rang} \mathcal{J}_{F_j}(\mathbf{c}^{(0)}) = n$, $j = 1, \ldots, m-1$, то система (14) имеет единственное решение и сложность S его нахождения алгоритмом равна

$$S = T_0 + \mathrm{O}(n^3(m-1)).$$

Используя предложенный алгоритм, можно решать системы ВКП-уравнений над произвольным кольцом вычетов $\mathbb{Z}_k$, $k > 1$. Напомним, что задачу решения систем полиномиальных уравнений над кольцом вычетов $\mathbb{Z}_k$ можно свести к решению систем полиномиальных уравнений над его соответствующими примарными компонентами. Аналогичным образом можно решать и системы ВКП-уравнений над $\mathbb{Z}_k$

$$\begin{cases} f_1(\mathbf{x}) = y_1, \\ \qquad \vdots \\ f_l(\mathbf{x}) = y_l, \end{cases}$$

где $y_i \in \mathbb{Z}_k$; $f_i \in \mathcal{CP}_k(n)$, $i = 1, \ldots, l$. Для этого в соответствии с определением 6 нужно перейти к функциям $f_{ij}(\mathbf{x}) \equiv f_i(\mathbf{x}) \pmod{p_j^{m_j}}$, где $k = p_1^{m_1} \cdot \ldots \cdot p_t^{m_t}$, и решить методом покоординатной линеаризации системы ВКП-уравнений

$$\begin{cases} f_{1j}(\mathbf{x}) = y_{1j}, \\ \qquad \vdots \\ f_{lj}(\mathbf{x}) = y_{lj} \end{cases}$$

над примарными компонентами $\mathbb{Z}_{p_j^{m_j}}$ ($y_{ij} \equiv y_i \pmod{p_j^{m_j}}$, $j = 1, \ldots, t$, $i = 1, \ldots, l$), после чего найти искомое решение над $\mathbb{Z}_k$.

Заключение

В работе введено и обобщено (по сравнению с [2, 3]) понятие функции с вариационно-координатной полиномиальностью на произвольное кольцо вычетов. Показано, что в общем случае данный класс расширяет класс полиномиальных функций, приведены оценки его мощности. Обобщён метод покоординатной линеаризации для решения систем уравнений, составленных из таких функций.

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. №1. С. 21–51.
2. *Заец М. В., Никонов В. Г., Шишков А. Б.* Класс функций с вариационно-координатной полиномиальностью над кольцом $\mathbb{Z}_{2^m}$ и его обобщение // Математические вопросы криптографии. 2013. Т. 4. №3. С. 19–45.
3. *Заец М. В., Никонов В. Г., Шишков А. Б.* Функции с вариационно-координатной полиномиальностью и их свойства // Открытое образование. 2012. №3. С. 57–61.
4. *Глухов М. М., Шишков А. Б.* Математическая логика. Дискретные функции. Теория алгоритмов. М.: Лань, 2012. 400 с.
5. *Anashin V. and Khrennikov A.* Applied Algebraic Dynamics. Berlin, N. Y.: Walter de Gruyter, 2009. 533 p.
6. *Hungerbuhler N. and Specker E.* A generalization of the Smarandache function to several variables // Integers. 2006. V. 6. P. 1–14.

7. *Заец М. В.* Решение систем ВКП-уравнений методом покоординатной линеаризации над примарным кольцом вычетов // Тезисы XLI Междунар. конф., XI Междунар. конф. молодых учёных «Информационные технологии в науке, образовании, телекоммуникации и бизнесе IT+SE13». Вестник Московского университета им. С. Ю. Витте. 2013. Сер. 1 (приложение). С. 155–157.