SystemVerilog Assertios of SystemVerilog-2009

Galina Alexanrovna Yaitskova, Candidate of Technical Sciences, Senior research associate
Research Institute of System Researches of Russian Academy of Sciences

The internal SystemVerilog Assertion of SystemVerilog-2009 order as a way of informational safety ensuring with using of assertions tools is presented.

Keywords: assertion, sequence, property, synchronized sequence.

УДК 519.716.32+519.854

КООРДИНАТНО-ЛИНЕЙНО РАЗРЕШИМЫЕ ФУНКЦИИ НАД ПРИМАРНЫМ КОЛЬЦОМ ВЫЧЕТОВ И МЕТОД ПОКООРДИНАТНОЙ ЛИНЕАРИЗАЦИИ

***Мирослав Владимирович Заец**, сотрудник*
Тел.:(916) 475-31-06, e-mail: mirzaets@hotmail.com
Федеральное государственное унитарное предприятие «Научно-исследовательский институт «Квант» ФГУП «НИИ КВАНТ»
www.rdi-kvant.ru

В статье рассматриваются и изучаются свойства нового класса функций над примарным кольцом вычетов, который обобщает класс полиномиальных функций и определенный ранее класс функций с вариационно-координатной полиномиальностью в работах [1], [2], [3]. Данные классы функций обладают тем свойством, что системы уравнений, составленные из таких функций, могут быть решены методом покоординатной линеаризации ([4], [5]).

Ключевые слова: функции с вариационно-координатной полиномиальностью, функции с координатно-линейной разрешимостью, полиномиальные функции, системы линейных уравнений, метод покоординатной линеаризации.

Введение

Известно, что системы полиномиальных уравнений над кольцом Галуа-Эйзенштейна (т.е. конечным коммутативным цепным кольцом) могут быть решены методом покоординатной линеаризации [5; 4]). 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 $GF(p)$. В статьях [1; 2] было показано, что класс функций над кольцом вычетов $\mathbb{Z}_{2^m}$, обладающий таким свойством, шире класса полиномиальных при $m \geq 3$. Построенный класс был назван классом «вариационно-координатно полиномиальных функций» (ВКП-функций). В данной работе определяется расширение класса ВКП-функций (и как следствие, полиномиальных), а именно класс функций с координатно-линейной разрешимостью (КЛР-функций). Приводятся свойства введенного класса, а также описывается метод покоординатной линеаризации для решения систем уравнений, составленных из таких функций.

М.В. Заец

1. Определение и свойства координатно-линейно разрешимых функций

Обозначим класс всех полиномиальных функций от $n \in \mathbb{N}$ переменных над кольцом $\mathbb{Z}_{p^m}$ через $\boldsymbol{\mathcal{P}}_{p^m}(n)$. Договоримся функции от переменных $x_1, \dots, x_n$ записывать кратко $f(\mathbf{x}) = f(x_1, \dots, x_n)$, класс всех функций от n переменных над кольцом вычетов

$\mathbb{Z}_{p^m}$ обозначим $\boldsymbol{\mathcal{F}}_{p^m}(n)$. Также всюду далее считаем, если не оговорено иное, что m, n - произвольные натуральные числа и $m > 1$. Отрезок множества целых чисел $\{t, t+1, \dots, s\}$ будем обозначать через $\overline{t,s}$.

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

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

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

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

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 $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{Z}_{p^m}^n$ однозначно представляется в виде конечной суммы:

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

где $\mathbf{x}^{(j)} = \left(x_1^{(j)}, \dots, x_n^{(j)}\right) \in \mathcal{B}^n, \ j = \overline{0, m-1}$.

Если при этом ввести на $\mathcal{B}$ операции сложения «$\oplus$» и умножения «$\otimes$» по правилу:

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

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

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

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

для всех $\alpha \in \mathbb{Z}_{p^m}^n$, будем называть ее j −ой координатной функцией, или j −ым координатным отображением.

Другими словами, любая функция $f(\mathbf{x}) \in \boldsymbol{\mathcal{F}}_{p^m}(n)$ представима следующим образом через свои координатные функции:

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

При этом любую координатную функцию $\gamma_j f, \ j = \overline{0, m-1}$, 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 $\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(m-1)}$. В таком случае будем предполагать, что координаты переменных расположены в указанном порядке, т.е. $\gamma_j f = \gamma_j f\big(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(m-1)}\big)$. Следовательно, любая такая координатная функция может быть представлена многочленом над полем $\mathcal{B}$ от указанных переменных.

Определение 2. *Функцию $f(\mathbf{x}) \in \boldsymbol{\mathcal{F}}_{p^m}(n)$ будем называть T-функцией, или треугольной функцией, если для любого $j \in \overline{0, m-1}$ ее j-ая координатная функция зависит только от координат переменных $\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j)}$, т.е. $\gamma_j f(\mathbf{x}) = \gamma_j f\big(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j)}\big)$.*

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

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

Обозначим через $\boldsymbol{\mathcal{D}}_{p^m}(n)$ – 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 $f \in \boldsymbol{\mathcal{P}}_{p^m}(n)$ сохраняет отношение сравнимости по любому делителю p^m, и поэтому справедливо включение

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

Следующая теорема устанавливает связь между классом треугольных функций и классом $\boldsymbol{\mathcal{D}}_{p^m}(n)$. Ее доказательство несложно получить, используя работу [6].

Теорема 1. *Пусть $f(\mathbf{x}) \in \boldsymbol{\mathcal{F}}_{p^m}(n)$, равносильны утверждения:*

1) $f(\mathbf{x}) \in \boldsymbol{\mathcal{D}}_{p^m}(n)$;

2) $f(\mathbf{x})$ является Т-функцией.

Определение 5. *Функцию $f(\mathbf{x}) \in \boldsymbol{\mathcal{F}}_{p^m}(n)$ назовем вариационно-координатно полиномиальной (или ВКП-функцией), если для любого $j \in \overline{0, m-1}$ существует полиномиальная функция $p_j(\mathbf{x}) \in \boldsymbol{\mathcal{P}}_{p^m}(n)$, $j-$ая координатная функция которой совпадает с $j-$ой координатной функцией функции $f(\mathbf{x})$, т.е. выполняется равенство:*

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

Класс всех ВКП-функций от n переменных над $\mathbb{Z}_{p^m}$ обозначим через $\boldsymbol{\mathcal{CP}}_{p^m}(n)$. Класс ВКП-функций в случае кольца вычетов $\mathbb{Z}_{2^m}$ был введен и изучался в работах [1; 2].

Из определения очевидным образом следует, что справедливо включение

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

Сформулируем основные свойства ВКП-функций без доказательства, которые далее нам пригодятся.

Теорема 2. *Справедливы утверждения:*

1) для любого $n \in \mathbb{N}$ классы полиномиальных и ВКП-функций над $\mathbb{Z}_{p^2}$ от n переменных совпадают, т.е. $\boldsymbol{\mathcal{P}}_{p^2}(n) = \boldsymbol{\mathcal{CP}}_{p^2}(n)$, при этом мощность данных классов равна величине:

$$\left|\boldsymbol{\mathcal{P}}_{p^2}(n)\right| = \left|\boldsymbol{\mathcal{CP}}_{p^2}(n)\right| = p^{p^n(n+2)};$$

2) для любых $n \in \mathbb{N}$ и $m \geq 3$ класс ВКП-функций $\boldsymbol{\mathcal{CP}}_{p^m}(n)$ не совпадает с классом полиномиальных $\boldsymbol{\mathcal{P}}_{p^m}(n)$.

Теорема 3. *При любом $n \in \mathbb{N}$ класс ВКП-функций $\boldsymbol{\mathcal{CP}}_{p^m}(n)$ сохраняет отношение сравнимости по любому делителю p^m, т.е. справедливо включение:*

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

Теорема 4. *Если $f \in \boldsymbol{\mathcal{CP}}_{p^m}(n)$, то для любого $j \in \overline{1, m-1}$ существуют функции $g_{ji}: \mathcal{B}^n \to \mathcal{B}$, $g_j: \mathcal{B}^{jn} \to \mathcal{B}$, $i = \overline{1, n}$, над полем $\mathcal{B}$ такие, что выполнено равенство:*

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

Класс ВКП-функций можно обобщить следующей конструкцией.

Определение 6. *Функцию $f(\mathbf{x}) \in \boldsymbol{\mathcal{F}}_{p^m}(n)$ назовем квази-вариационно-координатно полиномиальной (или квази-ВКП-функцией), если выполнены условия:*

1. $\gamma_0 f(\mathbf{x}) = \gamma_0 f\left(\mathbf{x}^{(0)}\right) = g_0\left(\mathbf{x}^{(0)}\right)$, $g_0: \mathcal{B}^n \to \mathcal{B}$; для любого $j \in \overline{1, m-1}$: 2 .

2. $\gamma_j f(\mathbf{x}) = \gamma_j f\left(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j)}\right)$ и существуют полиномиальные функции $g_{ji}: \mathcal{B}^n \to \mathcal{B}$, $g_j: \mathcal{B}^{jn} \to \mathcal{B}$, $i = \overline{1, n}$, над полем $\mathcal{B}$ такие, что справедливо равенство:

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

Введенное определение задает класс функций, обладающих свойством ВКП-функций, описанным в теореме 4. Класс всех квази-ВКП-функций от n переменных над кольцом $\mathbb{Z}_{p^m}$ обозначим $\boldsymbol{\mathcal{QCP}}_{p^m}(n)$. Как видно из определения следует, что любая квази-ВКП-функция является Т-функцией, поэтому справедлива цепочка включений:

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

Описание класса ВКП-функций носит конструктивный характер, поскольку в явном виде предлагает задание функций из этого класса. При этом важное свойство, которым обладают данные функции, описывается в теореме 4, а именно, оно заключается в том, что каждая j-ая координатная функция ($j\geq 1$) ВКП-функции является аффинной по j-тым координатам переменных (при фиксированных координатах меньшего порядка). И указанное свойство является ключевым при решении систем ВКП-уравнений, т.е. систем вида:

$$\begin{cases} f_1(\mathbf{x})=y_1,\\ \vdots\\ f_t(\mathbf{x})=y_t, \end{cases}$$

где $f_i(\mathbf{x})\in\boldsymbol{\mathcal{CP}}_{p^m}(n),\ y_i\in\mathbb{Z}_{p^m},\ i=\overline{1,t}$. Поэтому интересным представляется вопрос об описании всех функций над примарным кольцом $\mathbb{Z}_{p^m}$, которые им обладают, поскольку системы уравнений, левые части которых образованы такими функциями, могут быть решены «покоординатно». В данной статье будет предложен в некотором смысле аксиоматический подход к определению функций, имеющих описанное свойство.

Определение 7. *Функцию $f(\mathbf{x})\in\boldsymbol{\mathcal{F}}_{p^m}(n)$ назовем координатно $\mathcal{L}$-линейно разрешимой (или $\mathcal{L}$-КЛР-функцией), $\mathcal{L}\subseteq\overline{0,m-1}$, если она является Т-функцией и при любом $j\neq 0\in\mathcal{L}$ существуют такие функции $g_{ji},g_j\colon\mathcal{B}^{nj}\to\mathcal{B},\ i=\overline{1,n}$, что:*

$$\gamma_j f(\mathbf{x})=\gamma_j f\left(\mathbf{x}^{(0)},\dots,\mathbf{x}^{(j)}\right)=$$

$$=\sum_{i=1}^{n} g_{ji}\left(\mathbf{x}^{(0)},\dots,\mathbf{x}^{(j-1)}\right)\otimes x_i^{(j)}\oplus g_j\left(\mathbf{x}^{(0)},\dots,\mathbf{x}^{(j-1)}\right), \qquad (1)$$

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

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

При заданном подмножестве $\mathcal{L}\subseteq\overline{0,m-1}$ обозначим класс всех $\mathcal{L}$-КЛР-функций от n переменных над $\mathbb{Z}_{p^m}$ через $\boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}}(n)$, и при этом в условиях определения 6 будем также говорить, что функция $f(\mathbf{x})$ обладает свойством координатной $\mathcal{L}$-линейной разрешимости. В том случае, когда нам неважно множество $\mathcal{L}$ либо оно определено контекстом, будем говорить просто о КЛР-функциях и свойстве координатно-линейной разрешимости.

Введенный класс функций обобщает классы ВКП и квази-ВКП-функций, поскольку в нем условие, налагаемое на функцию g_{ji} менее жесткое – функция g_{ji} может зависеть от всех координат меньшего порядка, а не только от младших $\mathbf{x}^{(0)}$. При этом отметим, что для $\mathcal{L}$-КЛР-функции, при $j\in\overline{0,m-1}\backslash\mathcal{L}$ существует функция $g_j\colon\mathcal{B}^{n(j+1)}\to\mathcal{B}$, для которой:

$$\gamma_j f(\mathbf{x})=\gamma_j f\left(\mathbf{x}^{(0)},\dots,\mathbf{x}^{(j)}\right)=g_j\left(\mathbf{x}^{(0)},\dots,\mathbf{x}^{(j)}\right).$$

Приведем простейшие свойства $\mathcal{L}$-КЛР-функций в следующем утверждении.

Утверждение 5. *Справедливы утверждения:*

1. *если* $\mathcal{L} = \emptyset$, *то верно равенство:*

$$\boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}}(n) = \boldsymbol{\mathcal{D}}_{p^m}(n);$$

2. *если* $\mathcal{L}_1 \subseteq \mathcal{L}_2$, *то верно включение:*

$$\boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}_2}(n) \subseteq \boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}_1}(n);$$

3. *при любом* $\mathcal{L} \subseteq \overline{0, m-1}$ *верно включение:*

$$\boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}}(n) \subseteq \boldsymbol{\mathcal{D}}_{p^m}(n);$$

4. *если* $\mathcal{L}_1, \mathcal{L}_2 \subseteq \overline{0, m-1}$, *то верно равенство:*

$$\boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}_1}(n) \cap \boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}_2}(n) = \boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}_1 \cup \mathcal{L}_2}(n);$$

5. *если* $\mathcal{L}_1, \mathcal{L}_2 \subseteq \overline{0, m-1}$, *то верно включение:*

$$\boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}_1}(n) \cup \boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}_2}(n) \subseteq \boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}_1 \cap \mathcal{L}_2}(n).$$

Доказательство. 1. Из определения 7 следует, что при $\mathcal{L} = \emptyset$ все $\mathcal{L}$-КЛР-функции суть в точности Т-функции.

2. Если $\mathcal{L}_1 \subseteq \mathcal{L}_2$ и $f(\mathbf{x}) \in \boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}_2}(n)$, то при любом $j \in \mathcal{L}_1$ для ее j-ой координатной функции выполняется равенство вида (1), а значит, $f(\mathbf{x}) \in \boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}_1}(n)$.

3. При любом $\mathcal{L} \subseteq \overline{0, m-1}$ $\mathcal{L}$-КЛР-функции является Т-функцией, и включение заведомо выполнено. Кроме того, это также следует из первых двух пунктов, поскольку $\emptyset \subseteq \mathcal{L}$.

4. Пусть $\mathcal{L}_1, \mathcal{L}_2 \subseteq \overline{0, m-1}$ и $f(\mathbf{x}) \in \boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}_1}(n) \cap \boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}_2}(n)$, тогда j-ая координатная функция функции $f(\mathbf{x})$ удовлетворяет равенству (1) при $j \in \mathcal{L}_1$ и при $j \in \mathcal{L}_2$, а стало быть, при $j \in \mathcal{L}_1 \cup \mathcal{L}_2$. Обратно, если $f(\mathbf{x}) \in \boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}_1 \cup \mathcal{L}_2}(n)$, то ее тогда j-ая координатная функция удовлетворяет равенству (1) при всех $j \in \mathcal{L}_1$ и при всех $j \in \mathcal{L}_2$.

5. Доказываемое следует из второго пункта, так как $\mathcal{L}_1 \cap \mathcal{L}_2 \subseteq \mathcal{L}_i, i \in \{1,2\}$.

При любом $\mathcal{L} \subseteq \overline{0, m-1}$, как легко видеть, справедливо:

$$\boldsymbol{\mathcal{P}}_{p^m}(n) \cap \boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}}(n) \neq \emptyset,$$
$$\boldsymbol{\mathcal{CP}}_{p^m}(n) \cap \boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}}(n) \neq \emptyset, \quad \boldsymbol{\mathcal{QCP}}_{p^m}(n) \cap \boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}}(n) \neq \emptyset.$$

Уточним связь между классами полиномиальных, ВКП-, квази-ВКП- и $\mathcal{L}$-КЛР-функций в одном частном случае.

Утверждение 6. *Если* $\mathcal{L} \subseteq \overline{1, m-1}$, *то справедлива цепочка включений:*

$$\boldsymbol{\mathcal{P}}_{p^m}(n) \subseteq \boldsymbol{\mathcal{CP}}_{p^m}(n) \subseteq \boldsymbol{\mathcal{QCP}}_{p^m}(n) \subseteq \boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}}(n). \qquad (2)$$

Доказательство. В силу теоремы 4 и определения 6 любая ВКП-функция и квази-ВКП-функция является $\overline{1, m-1}$-КЛР-функцией, поэтому при $\mathcal{L} \subseteq \overline{1, m-1}$ цепочка (2) следует из п.2 утверждения 5.■

В силу цепочки (2) возникает вопрос о строгости включения классов $\boldsymbol{\mathcal{CP}}_{p^m}(n)$ и $\boldsymbol{\mathcal{QCP}}_{p^m}(n)$ в класс $\boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}}(n)$ при $\mathcal{L} \subseteq \overline{1, m-1}$. Ответ на него очевиден при $\mathcal{L} \subsetneq \overline{1, m-1}$ и при $\mathcal{L} = \overline{1, m-1}, m \geq 3$. Действительно, если $\mathcal{L} \subsetneq \overline{1, m-1}$, то

$$\boldsymbol{\mathcal{CP}}_{p^m}(n) \subseteq \boldsymbol{\mathcal{QCP}}_{p^m}(n) \subseteq \boldsymbol{\mathcal{CLS}}_{p^m}^{\overline{1,m-1}}(n) \subsetneq \boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}}(n).$$

И если $\mathcal{L} = \overline{1, m-1}$, $m \geq 3$, то по теореме 4 и определению 6 у ВКП- и квази-ВКП-функций все функции g_{ji} несущественно зависят от $x_1^{(k)}, \dots, x_n^{(k)}$, где $k = \overline{1, j-1}$, $j \geq 2$. В то же время, при $m \geq 3$ легко привести пример координатных функций $\gamma_j f$, $j \geq 2$, удовлетворяющих условиям определения 7, у которых g_{ji} существенно зависят хотя бы от одной из переменных $x_1^{(k)}, \dots, x_n^{(k)}$, где $k \in \overline{1, j-1}$. Поэтому и в этом случае имеем строгое включение:

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

Пример. Рассмотрим {0,1,2}-КЛР-функцию $f(x)$ от одной переменной над $\mathbb{Z}_{27}$ (см. табл.).

Таблица

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
5	**15**	**25**	**17**	**18**	**4**	**20**	**3**	**10**	**23**	**6**	**16**	**8**	**9**	**22**	**2**	**12**	**19**	**14**	**24**	**7**	**26**	**0**	**13**	**11**	**21**	**1**

Ее координатные функции имеют вид:

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

Такая функция не является полиномиальной, поскольку $g_{21}\left(x^{(0)}, x^{(1)}\right) = \left(x^{(1)}\right)^2 \oplus 2 \otimes x^{(1)} \oplus 2$ – существенно зависит от $x^{(1)}$. По этой же причине она не является и ВКП-функцией. Заметим, что эта функция также задает подстановку на $\mathbb{Z}_{27}$.

Остается рассмотреть случай $\mathcal{L} = \overline{1, m-1}$, $m = 2$. Для этого решим сначала вопрос о мощности класса $\mathcal{L}$-КЛР-функций. Предварительно докажем следующую лемму.

Лемма 7. *Число различных функций* $f(x_1, \dots, x_k, y_1, \dots, y_l): \mathcal{B}^{k+l} \to \mathcal{B}$ *от* $k + l$ *переменных над полем* $\mathcal{B}$ *вида*

$$f(x_1, \dots, x_k, y_1, \dots, y_l) = a_0(x_1, \dots, x_k) \oplus a_1(x_1, \dots, x_s) \otimes y_1 \oplus \dots \oplus a_l(x_1, \dots, x_s) \otimes y_l,$$

где $k, l \in \mathbb{N}$, $s \in \overline{1, k}$ *и* a_i, $i = \overline{0, l}$, *- произвольные функции над полем* $\mathcal{B}$, *равно* $p^{l \cdot p^s + p^k}$.

Доказательство. Очевидно, что разным наборам функций

$$\left(a_0(x_1, \dots, x_k), a_1(x_1, \dots, x_s), \dots, a_l(x_1, \dots, x_s)\right)$$

соответствуют различные функции $f(x_1, \dots, x_k, y_1, \dots, y_l)$. Следовательно, между такими наборами функций и функциями, имеющими вид из условия леммы, существует взаимно-однозначное соответствие. Число же указанных наборов равно в точности $p^{p^k} \cdot \left(p^{p^s}\right)^l = p^{l \cdot p^s + p^k}$.

Теорема 8. *Пусть* $\mathcal{L} = \{j_1, \dots, j_k\} \subseteq \overline{0, m-1}$, $k \in \overline{0, m}$, *и* $\{i_1, \dots, i_{m-k}\} = \overline{0, m-1} \backslash \mathcal{L}$. *Тогда для любого* $n \in \mathbb{N}$ *справедливо равенство*

$$\log_p \left|\boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}}(n)\right| = (n+1) \sum_{s=1}^{k} p^{n j_s} + \sum_{t=1}^{m-k} p^{(i_t+1)n}. \qquad (3)$$

Доказательство. Число всех $\mathcal{L}$-КЛР-функций равно произведению чисел возможных j −тых координатных отображений ($j = \overline{0, m-1}$). По определению 7 при каждом $j \in \mathcal{L}$ количество различных j −тых координатных отображений равно количеству функций вида

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

и равно, согласно доказанной лемме, $p^{np^{jn}+p^{jn}} = p^{(n+1)p^{jn}}$ (эта формула верна и в случае $j=0$). При каждом $j \in \overline{0,m-1}\backslash\mathcal{L}$ количество различных j −тых координатных отображений равно числу функций $g_j\left(\mathbf{x}^{(0)},\dots,\mathbf{x}^{(j)}\right)$ над полем $\mathcal{B}$ и равно $p^{p^{(j+1)n}}$.

Таким образом, имеем:

$$\left|\mathcal{CLS}_{p^m}^{\mathcal{L}}(n)\right| = \prod_{s=1}^{k} p^{(n+1)p^{j_s n}} \cdot \prod_{t=1}^{m-k} p^{p^{(i_t+1)n}} = p^{(n+1)\sum_{s=1}^{k} p^{j_s n}+\sum_{t=1}^{m-k} p^{(i_t+1)n}}.$$

Окончательно получим:

$$\log_p\left|\mathcal{CLS}_{p^m}^{\mathcal{L}}(n)\right| = (n+1)\sum_{s=1}^{k} p^{nj_s} + \sum_{t=1}^{m-k} p^{(i_t+1)n}.$$

Отметим, что в приведенной формуле (3) возможны равенства $k=0$ и $k=m$, в таких случаях первое и второе слагаемое соответственно в ней будут отсутствовать. При $\mathcal{L}=\emptyset$ и при $\mathcal{L}=\overline{1,m-1}$ получим два важных следствия.

Следствие. *Для любого $n \in \mathbb{N}$ мощность класса Т-функций $\mathcal{D}_{p^m}(n)$ вычисляется по формуле:*

$$\left|\mathcal{D}_{p^m}(n)\right| = p^{\frac{p^n(p^{nm}-1)}{p^n-1}}.$$

Доказательство. Так как $\mathcal{L}=\emptyset$, то $k=0$ и по формуле (3) имеем:

$$\log_p\left|\mathcal{D}_{p^m}(n)\right| = \log_p\left|\mathcal{CLS}_{p^m}^{\emptyset}(n)\right| = \sum_{i=0}^{m-1} p^{(i+1)n} = \frac{p^n(p^{nm}-1)}{p^n-1}.$$

Отсюда

$$\left|\mathcal{D}_{p^m}(n)\right| = p^{\frac{p^n(p^{nm}-1)}{p^n-1}}.$$

Следствие. *Для любого $n \in \mathbb{N}$ мощность класса $\mathcal{L}$-КЛР-функций при $\mathcal{L}=\overline{1,m-1}$ равна:*

$$\left|\mathcal{CLS}_{p^m}^{\mathcal{L}}(n)\right| = p^{p^n+(n+1)\frac{p^n\left(p^{n(m-1)}-1\right)}{p^n-1}}. \qquad (4)$$

Доказательство. Пользуясь формулой (3) непосредственно получим:

$$\log_p\left|\mathcal{CLS}_{p^m}^{\mathcal{L}}(n)\right| = (n+1)\sum_{j=1}^{m-1} p^{nj} + p^n = (n+1)\frac{p^n\left(p^{n(m-1)}-1\right)}{p^n-1} + p^n.$$

Применяя лемму 7, можно вычислить мощность класса квази-ВКП-функций.

Теорема 8. *Для любого $n \in \mathbb{N}$ мощность класса квази-ВКП-функций от n переменных над $\mathbb{Z}_{p^m}$ равна:*

$$\left|\mathcal{QCP}_{p^m}(n)\right| = p^{p^n+(m-1)n\cdot p^n+\frac{p^n\left(p^{n(m-1)}-1\right)}{p^n-1}}. \qquad (5)$$

Доказательство. Число всех квази-ВКП-функций равно произведению чисел возможных j −тых координатных отображений ($j=\overline{0,m-1}$). При каждом $j \in \overline{1,m-1}$ количество различных j −тых координатных отображений равно количеству функций вида

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

и равно, согласно доказанной лемме, $p^{np^n+p^{jn}}$. И при $j=0$ количество различных j −тых координатных отображений равно числу функций $g_j(\mathbf{x}^{(0)})$ над полем $\mathcal{B}$ и равно p^{p^n}.

В итоге имеем:

$$\left|\boldsymbol{\mathcal{QCP}}_{p^m}(n)\right| = p^{p^n}\prod_{j=1}^{m-1} p^{np^n+p^{jn}} = p^{p^n+(m-1)n\cdot p^n+\frac{p^n\left(p^{n(m-1)}-1\right)}{p^n-1}}.$$

Отметим, что равенство (5) дает оценку мощности класса ВКП-функций.

Используя доказанные результаты, можно окончательно ответить на вопрос о соотношении классов $\mathcal{L}$-КЛР и ВКП-функций.

Теорема 9. *Пусть $\mathcal{L}=\overline{1,m-1}$, тогда справедливы утверждения.*

1. При $m\geq 3$ верна цепочка включений:

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

2. Верна цепочка равенств:

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

Доказательство. При $m\geq 3$ данный факт уже доказан. При $m=2$ равенство следует из цепочки включений (2):

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

и равенства мощностей:

$$\left|\boldsymbol{\mathcal{P}}_{p^2}(n)\right|=\left|\boldsymbol{\mathcal{CP}}_{p^2}(n)\right|=\left|\boldsymbol{\mathcal{CLS}}^{\mathcal{L}}_{p^2}(n)\right|=p^{p^n(n+2)},$$

поскольку из (4) следует:

$$\left|\boldsymbol{\mathcal{CLS}}^{\mathcal{L}}_{p^2}(n)\right|=p^{p^n+(n+1)\frac{p^n(p^n-1)}{p^n-1}}=p^{p^n+(n+1)p^n}=p^{p^n(n+2)}.$$

В соответствии с определением 7, любая $\mathcal{L}$-КЛР-функция $f(\mathbf{x})$ сохраняет отношение сравнимости по делителям p^m, поэтому данное условие является необходимым для принадлежности произвольной функции классу $\boldsymbol{\mathcal{CLS}}^{\mathcal{L}}_{p^m}(n)$. Данное свойство не является достаточным в общем случае. Однако при $\mathcal{L}=\overline{1,m-1}$ оно является таковым для функций от одной переменной над $\mathbb{Z}_{2^m}$.

Утверждение 10. *Функция $f(x)\in\boldsymbol{\mathcal{F}}_{2^m}(1)$ является $\mathcal{L}$-КЛР-функцией, $\mathcal{L}=\overline{1,m-1}$, тогда и только тогда, когда она сохраняет отношение сравнимости по любому делителю 2^m. Другими словами, верно равенство:*

$$\boldsymbol{\mathcal{CLS}}^{\mathcal{L}}_{2^m}(1)=\boldsymbol{\mathcal{D}}_{2^m}(1).$$

Доказательство. Данное утверждение можно доказать аналогично теореме 9, используя мощностные соображения. Но в то же время его можно доказать непосредственной проверкой.

Пусть $f(x)\in\boldsymbol{\mathcal{D}}_{2^m}(1)$, докажем, что $f(x)\in\boldsymbol{\mathcal{CLS}}^{\mathcal{L}}_{2^m}(1)$. Согласно известным свойствам для любого $j\in\overline{0,m-1}$ справедливы следующие равенства:

$$\gamma_j f(x)=\gamma_j f\left(x^{(0)},\dots,x^{(j)}\right)=h_j\left(x^{(0)},\dots,x^{(j)}\right),$$

где $h_j\left(x^{(0)},\dots,x^{(j)}\right)\colon\mathcal{B}^{j+1}\to\mathcal{B}$ некоторая булева функция от $j+1$ переменных.

При $j\in\overline{1,m-1}$ булеву функцию $h_j\left(x^{(0)},\dots,x^{(j)}\right)$ можно однозначно представить в виде:

$$h_j\left(x^{(0)},\dots,x^{(j)}\right)=g_{j1}\left(x^{(0)},\dots,x^{(j-1)}\right)\cdot x^{(j)}+g_j\left(x^{(0)},\dots,x^{(j-1)}\right),$$

где g_{j1} и g_j – некоторые булевы функции, а это означает, что все $\gamma_j f(x) = h_j\left(x^{(0)}, \dots, x^{(j)}\right)$ имеют вид, указанный в определении 7, и $f(x) \in \boldsymbol{\mathcal{CLS}}_{2^m}^{\mathcal{L}}(1)$.

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

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

В действительности можно доказать, что справедливо определенное усиление утверждения 10.

Следствие. *Класс* $\mathcal{L}$*-КЛР-функцией* $\boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}}(n)$*,* $\mathcal{L} = \overline{1, m-1}$*, совпадает с классом Т-функций* $\boldsymbol{\mathcal{D}}_{p^m}(n)$ *тогда и только тогда, когда одновременно* $p = 2,\ n = 1$.

Следствие. *Класс ВКП-функцией* $\boldsymbol{\mathcal{CP}}_{p^m}(n)$*, совпадает с классом Т-функций* $\boldsymbol{\mathcal{D}}_{p^m}(n)$ *тогда и только тогда, когда одновременно* $p = 2,\ m = 2,\ n = 1$*. Это справедливо и для класса полиномиальных функций* $\boldsymbol{\mathcal{P}}_{p^m}(n)$.

Докажем далее определенную замкнутость класса КЛР-функций при применении суперпозиции.

Теорема 11. *Пусть* $\mathcal{L}_1, \mathcal{L}_2 \subseteq \overline{0, m-1},\ k, n \in \mathbb{N}$*. Если функции* $f \in \boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}_1}(n)$ *и* $h_1, \dots, h_n \in \boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}_2}(k)$*, то функция* $f(h_1, \dots, h_n) \in \boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}_1 \cap \mathcal{L}_2}(k)$.

Доказательство. Пусть $u(\mathbf{x}) = f\left(h_1(\mathbf{x}), \dots, h_n(\mathbf{x})\right)$, проверим, что $u(\mathbf{x})$ является Т-функцией. Действительно, при любом $j \in \overline{0, m-1}$:

$$\gamma_j u(\mathbf{x}) = \gamma_j f\left(h_1(\mathbf{x}), \dots, h_n(\mathbf{x})\right) = \gamma_j f\left(\gamma_0 h_1(\mathbf{x}), \dots, \gamma_0 h_n(\mathbf{x}), \dots, \gamma_j h_1(\mathbf{x}), \dots, \gamma_j h_n(\mathbf{x})\right).$$

Поскольку при любом $s \in \overline{0, j}$ и $i \in \overline{1, n}$ координатная функция $\gamma_s h_i(\mathbf{x})$ зависит от координат переменных $\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(s)}$, постольку j-ая координатная функция $\gamma_j u(\mathbf{x})$ зависит от координат $\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j)}$, а следовательно, $u(\mathbf{x})$ – Т-функция.

Если $\mathcal{L}_1 \cap \mathcal{L}_2 = \emptyset$, то утверждение верно в силу $\boldsymbol{\mathcal{CLS}}_{p^m}^{\emptyset}(k) = \boldsymbol{\mathcal{D}}_{p^m}(k)$. Если же $\mathcal{L}_1 \cap \mathcal{L}_2 \neq \emptyset$, то возьмем $j \neq 0 \in \mathcal{L}_1 \cap \mathcal{L}_2$ и рассмотрим j-ую координатную функцию $\gamma_j u(\mathbf{x})$. Обозначим через g_j^f, g_{ji}^f и $g_j^{h_l}, g_{ji}^{h_l}$ $(l = \overline{1, n})$ функции из определения 7 для f и h_l соответственно. Тогда имеем:

$$\gamma_j u(\mathbf{x}) = \gamma_j f\left(h_1(\mathbf{x}), \dots, h_n(\mathbf{x})\right) =$$

$$\sum_{i=1}^{n} g_{ji}^f\left(\gamma_0 h_1(\mathbf{x}), \dots, \gamma_0 h_n(\mathbf{x}), \dots, \gamma_{j-1} h_1(\mathbf{x}), \dots, \gamma_{j-1} h_n(\mathbf{x})\right) \otimes \gamma_j h_i(\mathbf{x}) \oplus$$

$$\oplus\, g_j^f\left(\gamma_0 h_1(\mathbf{x}), \dots, \gamma_0 h_n(\mathbf{x}), \dots, \gamma_{j-1} h_1(\mathbf{x}), \dots, \gamma_{j-1} h_n(\mathbf{x})\right).$$

По аналогии с отмеченным ранее, выражения

$$g_{ji}^f\left(\gamma_0 h_1(\mathbf{x}), \dots, \gamma_0 h_n(\mathbf{x}), \dots, \gamma_{j-1} h_1(\mathbf{x}), \dots, \gamma_{j-1} h_n(\mathbf{x})\right) = r_{ji}\left(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j-1)}\right)$$

и

$$g_j^f\left(\gamma_0 h_1(\mathbf{x}), \dots, \gamma_0 h_n(\mathbf{x}), \dots, \gamma_{j-1} h_1(\mathbf{x}), \dots, \gamma_{j-1} h_n(\mathbf{x})\right) = r_j\left(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j-1)}\right)$$

зависят только от $\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j-1)}$, следовательно:

$$\gamma_j u(\mathbf{x}) = \sum_{i=1}^{n} r_{ji}\left(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j-1)}\right) \otimes \gamma_j h_i(\mathbf{x}) \oplus r_j\left(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j-1)}\right) =$$

$$= \sum_{i=1}^{n} r_{ji}\left(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j-1)}\right) \otimes$$

$$\otimes\left(\sum_{s=1}^{k} g_{ji}^{h_i}\left(\mathbf{x}^{(0)},\dots,\mathbf{x}^{(j-1)}\right)\otimes x_s^{(j)}\oplus g_j^{h_i}\left(\mathbf{x}^{(0)},\dots,\mathbf{x}^{(j-1)}\right)\right)\oplus$$

$$\oplus\, r_j\left(\mathbf{x}^{(0)},\dots,\mathbf{x}^{(j-1)}\right)=$$

$$=\sum_{i=1}^{n} r_{ji}\left(\mathbf{x}^{(0)},\dots,\mathbf{x}^{(j-1)}\right)\otimes\left(\sum_{s=1}^{k} g_{ji}^{h_i}\left(\mathbf{x}^{(0)},\dots,\mathbf{x}^{(j-1)}\right)\otimes x_s^{(j)}\right)\oplus$$

$$\oplus\sum_{i=1}^{n} r_{ji}\left(\mathbf{x}^{(0)},\dots,\mathbf{x}^{(j-1)}\right)\otimes g_j^{h_i}\left(\mathbf{x}^{(0)},\dots,\mathbf{x}^{(j-1)}\right)\oplus r_j\left(\mathbf{x}^{(0)},\dots,\mathbf{x}^{(j-1)}\right)=$$

$$=\sum_{s=1}^{k}\left(\sum_{i=1}^{n} g_{ji}^{h_i}\left(\mathbf{x}^{(0)},\dots,\mathbf{x}^{(j-1)}\right)\otimes r_{ji}\left(\mathbf{x}^{(0)},\dots,\mathbf{x}^{(j-1)}\right)\right)\otimes x_s^{(j)}\oplus$$

$$\oplus\sum_{i=1}^{n} r_{ji}\left(\mathbf{x}^{(0)},\dots,\mathbf{x}^{(j-1)}\right)\otimes g_j^{h_i}\left(\mathbf{x}^{(0)},\dots,\mathbf{x}^{(j-1)}\right)\oplus r_j\left(\mathbf{x}^{(0)},\dots,\mathbf{x}^{(j-1)}\right).$$

После очевидных переобозначений, придем к равенству:

$$\gamma_j u(\mathbf{x})=\sum_{i=1}^{k} g_{ji}^{u}\left(\mathbf{x}^{(0)},\dots,\mathbf{x}^{(j-1)}\right)\otimes x_i^{(j)}\oplus g_j^{u}\left(\mathbf{x}^{(0)},\dots,\mathbf{x}^{(j-1)}\right).$$

Таким образом, каждая координатная функция $\gamma_j u(\mathbf{x})$, $j\neq 0\in\mathcal{L}_1\cap\mathcal{L}_2$, удовлетворяет условиям определения 7.

Если $j=0\in\mathcal{L}_1\cap\mathcal{L}_2$, то, применяя аналогичные рассуждения, получим:

$$\gamma_0 u(\mathbf{x})=\gamma_0 f\left(h_1(\mathbf{x}),\dots,h_n(\mathbf{x})\right)=\gamma_0 f\left(\gamma_0 h_1\left(\mathbf{x}^{(0)}\right),\dots,\gamma_0 h_n\left(\mathbf{x}^{(0)}\right)\right).$$

Функция $\gamma_0 f$ – аффинная над полем $\mathcal{B}$ и $\gamma_0 h_1\left(\mathbf{x}^{(0)}\right),\dots,\gamma_0 h_n\left(\mathbf{x}^{(0)}\right)$ – также аффинные над $\mathcal{B}$, их суперпозиция есть аффинная функция.

Таким образом, функция u является $\mathcal{L}_1\cap\mathcal{L}_2$-КЛР-функцией. ■

Из данной теоремы получим важное следствие. Пусть $\boldsymbol{\mathcal{K}}$ – некоторый класс функций, обозначим через $[\boldsymbol{\mathcal{K}}]$ - замыкание этого класса (состоящее из всех функций, представимых формулой над $\boldsymbol{\mathcal{K}}$, или что то же самое, содержащее все возможные суперпозиции функций из $\boldsymbol{\mathcal{K}}$). Класс функций $\boldsymbol{\mathcal{K}}$ называется замкнутым, если его замыкание $[\boldsymbol{\mathcal{K}}]$ совпадает с самим собой.

Следствие. *При любых* $n\in\mathbb{N}$ *и* $\mathcal{L}\subseteq\overline{0,m-1}$ *справедливо:*

$$\left[\boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}}(n)\right]=\boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}}(n).$$

Доказательство. Действительно, по доказанной теореме суперпозиция любых $\mathcal{L}$-КЛР-функций является снова $\mathcal{L}$-КЛР-функцией, отсюда и следует замкнутость класса $\boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}}(n)$.

В частности из следствия вытекает и замкнутость класса Т-функций при $\mathcal{L}=\emptyset$, т.е.

$$\left[\boldsymbol{\mathcal{D}}_{p^m}(n)\right]=\boldsymbol{\mathcal{D}}_{p^m}(n).$$

Повторяя доказательство теоремы 11, можно показать замкнутость класса квази-ВКП-функций.

Утверждение 12. *Если функция* $f\in\boldsymbol{\mathcal{QCP}}_{p^m}(n)$ *и функции* $h_1,\dots,h_n\in\boldsymbol{\mathcal{QCP}}_{p^m}(k)$, *то их суперпозиция* $f(h_1,\dots,h_n)\in\boldsymbol{\mathcal{QCP}}_{p^m}(k)$.

Следствие. *При любом* $n\in\mathbb{N}$ *справедливо:*

$$\left[\boldsymbol{\mathcal{QCP}}_{p^m}(n)\right]=\boldsymbol{\mathcal{QCP}}_{p^m}(n).$$

Суммируя полученные результаты, придем к следующему выводу. При $m\geq 3$, в соответствии с теоремой 9, имеем цепочку включений:

$$\boldsymbol{\mathcal{P}}_{p^m}(n) \subsetneq \boldsymbol{\mathcal{CP}}_{p^m}(n) \subseteq \boldsymbol{\mathcal{QCP}}_{p^m}(n) \subsetneq \boldsymbol{\mathcal{CLS}}_{p^m}^{\overline{1,m-1}}(n).$$

При этом классы $\boldsymbol{\mathcal{P}}_{p^m}(n)$, $\boldsymbol{\mathcal{QCP}}_{p^m}(n)$, $\boldsymbol{\mathcal{CLS}}_{p^m}^{\overline{1,m-1}}(n)$ являются замкнутыми и не совпадают. Открытым остается вопрос о замкнутости класса ВКП-функций и о строгости его включения в класс квази-ВКП-функций.

2. Метод покоординатной линеаризации для решения систем КЛР-уравнений

Как говорилось ранее, цель изучения класса КЛР-функций заключается в обобщении метода покоординатной линеаризации на более широкий класс функций. Изложение метода покоординатной линеаризации для решения систем ВКП-уравнений можно найти в работе [3]. Далее пойдет речь о решении систем $\mathcal{L}$-КЛР-уравнений над $\mathbb{Z}_{p^m}$ $(m > 1)$, т.е. систем

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

у которых функции $f_i(\mathbf{x})$, $i = \overline{1,t}$, стоящие в левой части каждого уравнения, являются $\mathcal{L}$-КЛР-функциями. Приводить алгоритм будем для случая, когда $\mathcal{L} = \overline{1,m-1}$. При таком $\mathcal{L}$ системы ВКП-уравнений являются системами $\mathcal{L}$-КЛР-уравнений.

Приведем соображения, которые будут использоваться при описании и обосновании алгоритма решения систем $\mathcal{L}$-КЛР-уравнений.

Если $f(\mathbf{x}) \in \boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}}(n)$ и $y \in \mathbb{Z}_{p^m}$, то уравнение $f(\mathbf{x}) = y$ после приведения его левой и правой частей по модулю p примет вид

$$f(\mathbf{x}) \equiv y \pmod p \Leftrightarrow \gamma_0 f(\mathbf{x}) = y^{(0)} \Leftrightarrow \gamma_0 f\left(\mathbf{x}^{(0)}\right) = y^{(0)}$$

Последнее равносильно уравнению над полем $\mathcal{B}$:

$$g_0\left(\mathbf{x}^{(0)}\right) = y^{(0)}.$$

При этом, чтобы найти функцию g_0 достаточно привести по модулю p значения функции $f(\mathbf{x})$ на множестве $\mathcal{B}^n$.

Если $f(\mathbf{x}) \in \boldsymbol{\mathcal{CLS}}_{p^m}^{\mathcal{L}}(n)$, $y \in \mathbb{Z}_{p^m}$ и $j \in \overline{0,m-2}$, то уравнение $f(\mathbf{x}) = y$ после приведения по модулю p^{j+1} примет вид:

$$f(\mathbf{x}) \equiv y \left(\mathrm{mod}\, p^{j+1}\right) \Leftrightarrow$$
$$\gamma_0 f(\mathbf{x}) + \cdots + p^j \gamma_j f(\mathbf{x}) = y^{(0)} + \cdots + p^j y^{(j)} \Leftrightarrow$$
$$\begin{cases} \gamma_0 f(\mathbf{x}) = y^{(0)}, \\ \gamma_1 f(\mathbf{x}) = y^{(1)}, \\ \vdots \\ \gamma_j f(\mathbf{x}) = y^{(j)}. \end{cases}$$

Поскольку при любом $s \in \overline{0,j}$ координатная функция $\gamma_s f(\mathbf{x})$ зависит только от $\mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(s)}$, то полученную систему можно записать следующим образом:

$$\begin{cases} \gamma_0 f\left(\mathbf{x}^{(0)}\right) = y^{(0)}, \\ \gamma_1 f\left(\mathbf{x}^{(0)}, \mathbf{x}^{(1)}\right) = y^{(1)}, \\ \vdots \\ \gamma_j f\left(\mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(j)}\right) = y^{(j)}. \end{cases} \quad (6)$$

Пусть координаты $\mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(j-1)}$ удовлетворяют первым j уравнениям (6), тогда для решения (6) необходимо и достаточно решить уравнение

$$\gamma_j f\left(\mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(j)}\right) = y^{(j)} \quad (7)$$

относительно $\mathbf{x}^{(j)}$. При этом (7) является линейным по $\mathbf{x}^{(j)}$ при любых фиксированных координатах $\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j-1)}$, поскольку, согласно свойству координатно-линейной разрешимости, уравнение (7) есть в точности уравнение вида

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

Алгоритм решения систем $\mathcal{L}$-КЛР-уравнений

Пусть задана система $\mathcal{L}$-КЛР-уравнений от n переменных $x_1, \dots, x_n$ при $\mathcal{L} = \overline{1, m-1}$

$$\begin{cases} f_1(\mathbf{x}) = y_1, \\ \vdots \\ f_l(\mathbf{x}) = y_l, \end{cases} \tag{8}$$

над $\mathbb{Z}_{p^m}$ $(m > 1)$, опишем алгоритм, приводящий к нахождению ее решений.

1. Положим $j = 0$. Рассмотрим произвольное уравнение системы

$$f_i(\mathbf{x}) = y_i, \qquad i \in \overline{1, l},$$

и приведем его по модулю p. Согласно проведенным ранее рассуждениям получим уравнение

$$\gamma_0 f_i\left(\mathbf{x}^{(0)}\right) = y_i^{(0)} \Leftrightarrow g_0^{f_i}\left(\mathbf{x}^{(0)}\right) = y_i^{(0)}$$

относительно младших координат $\mathbf{x}^{(0)}$. Приводя таким образом каждое уравнение в (8), придем к некоторой системе уравнений над полем $\mathcal{B}$ относительно $\mathbf{x}^{(0)}$. Решаем данную систему одним из стандартных способов (например, перебором) и находим возможные значения младших координат.

2. Пусть при $j \in \overline{1, m-1}$ найдены значения координат переменных $\mathbf{x}^{(0)} = \mathbf{c}^{(0)}, \dots, \mathbf{x}^{(j-1)} = \mathbf{c}^{(j-1)}$, которые для каждого уравнения $f_i(\mathbf{x}) = y_i$, $i = \overline{1, l}$, системы (8) удовлетворяют равенствам:

$$\begin{cases} \gamma_0 f_i\left(\mathbf{c}^{(0)}\right) = y_i^{(0)}, \\ \gamma_1 f_i\left(\mathbf{c}^{(0)}, \mathbf{c}^{(1)}\right) = y_i^{(1)}, \\ \vdots \\ \gamma_{j-1} f_i\left(\mathbf{c}^{(0)}, \dots, \mathbf{c}^{(j-1)}\right) = y_i^{(j-1)}. \end{cases} \tag{9}$$

Если $j = m$, то перейти к пункту 4. Иначе, при любом таком наборе координат неизвестных $\mathbf{c}^{(0)}, \dots, \mathbf{c}^{(j-1)}$ выполним следующие действия. Приведем данное уравнение по модулю p^{j+1}, получим соотношение

$$\gamma_j f_i\left(\mathbf{c}^{(0)}, \dots, \mathbf{c}^{(j-1)}, \mathbf{x}^{(j)}\right) = y_i^{(j)} \Leftrightarrow$$

$$\sum_{k=1}^{n} g_{jk}^{f_i}\left(\mathbf{c}^{(0)}, \dots, \mathbf{c}^{(j-1)}\right) \otimes x_k^{(j)} \oplus g_j^{f_i}\left(\mathbf{c}^{(0)}, \dots, \mathbf{c}^{(j-1)}\right) = y_i^{(j)}, \tag{10}$$

которое при любых фиксированных наборах значений $\mathbf{c}^{(0)}, \dots, \mathbf{c}^{(j-1)}$ является линейным. Это означает, что существуют такие $a_{jk}^{f_i}, a_j^{f_i} \in \mathcal{B}$ $(k = \overline{1, n})$, для которых (10) имеет вид:

$$a_{j1}^{f_i} \otimes x_1^{(j)} \oplus \dots \oplus a_{jn}^{f_i} \otimes x_n^{(j)} \oplus a_j^{f_i} = y_i^{(j)}.$$

Чтобы найти эти коэффициенты (при фиксированных $\mathbf{c}^{(0)}, \dots, \mathbf{c}^{(j-1)}$) достаточно вычислить значения $\gamma_j f_i\left(\mathbf{c}^{(0)}, \dots, \mathbf{c}^{(j-1)}, \mathbf{x}^{(j)}\right)$ как функции от $\mathbf{x}^{(j)}$ на наборах $\{\theta = (0, \dots, 0), \theta_i = (\delta_{i,1}, \dots, \delta_{i,n}), i = \overline{1, n}\}$. Таким образом, каждое уравнение исходной системы приводит к некоторому линейному уравнению над полем $\mathcal{B}$ относительно неизвестных $\mathbf{x}^{(j)}$. А значит, решив полученную систему линейных уравнений над $\mathcal{B}$, найдем возможные значения j-х координат переменных либо покажем, что такая система несовместна.

3. При всех $\mathbf{c}^{(0)}, \dots, \mathbf{c}^{(j-1)}$, удовлетворяющих системе (9), необходимо найти все возможные значения координат $\mathbf{x}^{(j)}$. Если таких $\mathbf{x}^{(j)}$ нет, то исходная система (8)

несовместна и алгоритм заканчивает работу. Увеличить j на 1 и перейти к пункту 2 алгоритма.

4. Если найдены координаты неизвестных $\mathbf{x}^{(0)} = \mathbf{c}^{(0)}, \dots, \mathbf{x}^{(m-1)} = \mathbf{c}^{(m-1)}$, то решения системы $\mathbf{c} = (c_1, \dots, c_n)$ находятся следующим образом:

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

и на этом алгоритм завершает работу.

Утверждение 13. *Приведенный алгоритм корректен, то есть находит все решения системы (8) либо определяет ее несовместность.*

Доказательство. Корректность алгоритма следует из того, что $\mathbf{c} = (c_1, \dots, c_n)$ является решением (8) в том и только в том случае, когда для любого уравнения этой системы $f_i(\mathbf{x}) = y_i,\ i = \overline{1,l}$, выполняются равенства

$$\begin{cases} \gamma_0 f_i(\mathbf{c}^{(0)}) = y_i^{(0)}, \\ \gamma_1 f_i(\mathbf{c}^{(0)}, \mathbf{c}^{(1)}) = y_i^{(1)}, \\ \vdots \\ \gamma_{m-1} f_i(\mathbf{c}^{(0)}, \dots, \mathbf{c}^{(m-1)}) = y_i^{(m-1)}. \end{cases}$$

Но данный алгоритм последовательно на каждом шаге находит все те значения координат $\mathbf{c}^{(0)}, \dots, \mathbf{c}^{(j)}$, которые удовлетворяют равенствам

$$\begin{cases} \gamma_0 f_i(\mathbf{c}^{(0)}) = y_i^{(0)}, \\ \gamma_1 f_i(\mathbf{c}^{(0)}, \mathbf{c}^{(1)}) = y_i^{(1)}, \\ \vdots \\ \gamma_j f_i(\mathbf{c}^{(0)}, \dots, \mathbf{c}^{(j)}) = y_i^{(j)}, \end{cases}$$

для любого уравнения $f_i(\mathbf{x}) = y_i$ исходной системы. В частности, при $j = m-1$ – все возможные значения координат переменных $\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(m-1)}$, а стало быть, и все решения $\mathbf{c} = (c_1, \dots, c_n)$.

Оценим сложность одного прохода алгоритма (п.2). Для нахождения координат $\mathbf{x}^{(j)}$ ($j \in \overline{1, m-1}$), как видно, требуется решить систему линейных уравнений над полем $\mathcal{B}$. В предположении, что в системе $l = O(n)$ уравнений, ее решение методом Гаусса имеет сложность $O(n^3)$. Кроме того, чтобы получить саму эту систему, необходимо найти линейное представление $a_{j1} \otimes x_1^{(j)} \oplus \dots \oplus a_{jn} \otimes x_n^{(j)} \oplus a_j = y^{(j)}$ для каждого ее уравнения. Очевидно, что для одного уравнения это можно сделать за $n+1$ операций (считая, что вычисление значения функции – это одна операция), и за $(n+1) \cdot O(n) = O(n^2)$ операций для всей системы. Таким образом, сложность одного прохода равна $O(n^3) + O(n^2) = O(n^3)$ (при $j \neq 0$).

Приведенный алгоритм решения систем $\overline{1, m-1}$-КЛР-уравнений можно обобщить на системы $\mathcal{L}$-КЛР-уравнений при произвольном $\mathcal{L} \subseteq \overline{0, m-1}$. В таком случае для нахождения j-ых координат, где $j \in \mathcal{L}$, потребуется решить систему линейных уравнений над полем $\mathcal{B}$ и для нахождения координат с номерами $j \in \overline{0, m-1} \backslash \mathcal{L}$ решить, вообще говоря, произвольную систему над полем $\mathcal{B}$. Этот факт объясняет используемую терминологию в названии функций: систему $\mathcal{L}$-КЛР-уравнений можно решить покоординатно, т.е. последовательно находя координаты неизвестных переменных, при этом координаты $j \in \mathcal{L}$ находятся путем решения системы линейных уравнений, отсюда и название – «функции с координатной $\mathcal{L}$-линейной разрешимостью».

Заключение

Автор считает, что в данной работе новыми являются следующие положения и результаты: классификация функций над примарным кольцом вычетов в связи с при-

менением метода покоординатной линеаризации и общее описание данного метода для класса функций с координатно-линейной разрешимостью. Изучение и исследование метода покоординатной линеаризации для решения систем полиномиальных уравнений позволило существенно расширить классы функций, обладающих данным свойством. Это привело к появлению определенной классификации таких функций над примарным кольцом вычетов, которая была приведена в настоящей статье. Также сам метод покоординатной линеаризации получил развитие и был обобщен на класс функций с координатно-линейной разрешимостью.

Литература

1. *Заец М.В., Никонов В.Г., Шишков А.Б.* Функции с вариационно-координатной полиномиальностью и их свойства // Открытое образование. 2012. № 3. С. 57-61.
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 // Матем. вопр. криптографии. 2013. Т. 4. № 3. С. 19-45.
3. *Заец М.В.* Решение систем ВКП-уравнений методом покоординатной линеаризации над примарным кольцом вычетов // Информационные технологии в науке, образовании, телекоммуникации и бизнесе: мат. XLI Международной конференции и XI Международной конференции молодых ученых IT+SE13. – приложение к журналу Вестник Московского университета имени С.Ю. Витте. Серия 1: Экономика и управление. 2013. С. 155-157.
4. *Михайлов Д.А.* Решение некоторых классов систем полиномиальных уравнений над конечными полями и кольцами: труды по дискретной математике. 2008. Т. 11. С. 125-146
5. *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.
6. *Vladimir Anashin* and *Andrei Khrennikov*. Applied Algebraic Dynamics. De Gruyter Expositions in Mathematics, vol. 49 Walter de Gruyter, Berlin‑New York, 2009.

Coordinate-linear solvable functions over primary ring of residues and the method of coordinate linearization

***Miroslav Vladimirovich Zayets**, Associate*
Federal State Unitary Enterprise KVANT Research Institute

The article considers and researches properties of the new class of functions over primary ring of residues, which generalizes class of polynomial functions and class of functions with variative-coordinate polynomiality defined earlier. The given classes of functions have the property that systems of equations composed from such functions may be solved by using the method of coordinate linearization.

Key words: functions with variative-coordinate polynomiality, coordinate-linear solvable functions, polynomial functions, system of linear equations, method of coordinate linearization.

УДК 681.51

ОЦЕНКА СТЕПЕНИ ВЛИЯНИЯ НЕКОТОРЫХ ФАКТОРОВ НА ПРОИЗВОДИТЕЛЬНОСТЬ LONWORKS СЕТИ

***Сергей Александрович Даденков**, ассистент кафедры «Автоматика и Телемеханика», Тел. (342) 239-18-16, e-mail: dadenkov@rambler.ru*
***Ефим Львович Кон**, канд.техн.наук, проф. кафедры «Автоматика и Телемеханика» Тел.: (342) 239-18-16, e-mail: kel-40@yandex.ru*
Пермский национальный исследовательский политехнический университет http://pstu.ru