Math-Net.Ru

Общероссийский математический портал

М. В. Заец, В. Г. Никонов, А. Б. Шишков, Класс функций с вариационно-координатной полиномиальностью над кольцом $\mathbb{Z}_{2^m}$ и его обобщение, *Матем. вопр. криптогр.*, 2013, том 4, выпуск 3, 21–47

DOI: <https://doi.org/10.4213/mvk91>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.234.156.22

26 апреля 2023 г., 10:20:26

**Класс функций
с вариационно-координатной
полиномиальностью над кольцом $\mathbb{Z}_{2^m}$
и его обобщение**

М. В. Заец¹, В. Г. Никонов², А. Б. Шишков³

^{1,3} ООО «Центр сертификационных исследований», Москва

² Академия криптографии Российской Федерации, Москва

Получено 11.IV.2012

В статье рассматриваются классы функций над кольцом вычетов $\mathbb{Z}_{2^m}$, порождающих системы уравнений, у которых нахождение $(i + 1)$ -х координат неизвестных при известных координатах меньшего порядка сводится к решению системы линейных уравнений.

Ключевые слова: функции над кольцом вычетов $\mathbb{Z}_{2^m}$, полиномиальные функции, системы полиномиальных уравнений, системы линейных уравнений

**A class of functions with coordinate-dependent polynomiality
over the ring $\mathbb{Z}_{2^m}$**

M. V. Zaec¹, V. G. Nikonov², F. B. Shishkov³

^{1,3} LCD “Certification Research Center”, Moscow

² Academy of Cryptography of the Russian Federation, Moscow

Abstract. We consider class of functions over the residue ring $\mathbb{Z}_{2^m}$ generating the systems of equations such that given the first i coordinates of unknowns the next $(i+1)^{\text{th}}$ coordinates may be found as the solution of system of linear equations.

Key words: functions over residue ring $\mathbb{Z}_{2^m}$, polynomial functions, systems of polynomial equations, systems of linear equations

Citation: *Mathematical Aspects of Cryptography*, 2013, vol. 4, no. 3, pp. 21–47 (Russian).

© 2013 М. В. Заец, В. Г. Никонов, А. Б. Шишков

Широкий класс задач дискретной математики сводится к анализу и решению систем уравнений над кольцами вычетов $\mathbb{Z}_k$:

$$\begin{cases} \dots \\ f_i(x_1, \dots, x_n) = y_i, \\ \dots \end{cases}$$

Особый интерес при этом представляет случай, когда $k = 2^m$ для некоторого $m \in \mathbb{N}$. Тогда, полагая $\mathcal{B} = \{0, 1\} \subseteq \mathbb{Z}_{2^m}$, любой элемент $a \in \mathbb{Z}_{2^m}$ можно представить в виде

$$a = a^{(0)} + 2 \cdot a^{(1)} + \dots + 2^{m-1} a^{(m-1)}, \quad a^{(j)} \in \mathcal{B}, \quad j = 0, \dots, m-1,$$

который называется разложением элемента a в двоичном координатном множестве $\mathcal{B}$. Отображения

$$\gamma_j: \mathbb{Z}_{2^m} \rightarrow \mathcal{B}, \quad \gamma_j(a) = a^{(j)}, \quad j = 0, \dots, m-1,$$

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

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

то алгебра $(\mathcal{B}, \oplus, \cdot)$ будет являться полем из двух элементов.

Напомним, что класс функций $\{x_1 \cdot x_2, x_1 + x_2, 1\}$ над $\mathbb{Z}_{2^m}$ (при $m > 1$) не является полным, т. е. не всякая функция $f(x_1, \dots, x_n): \mathbb{Z}_{2^m}^n \rightarrow \mathbb{Z}_{2^m}$ представима формулой над этим классом. Функции же, представимые формулой над указанным классом, или, что то же самое, представимые некоторым многочленом над $\mathbb{Z}_{2^m}$, получили название полиномиальных. Обозначим класс всех полиномиальных функций над $\mathbb{Z}_{2^m}$ от $n \in \mathbb{N}$ переменных через $\mathbf{P}_{2^m}(n)$.

Можно показать (см. [2, 3]), что система полиномиальных уравнений над $\mathbb{Z}_{2^m}$, т. е. уравнений, в которых функции $f_i(x_1, \dots, x_n)$ являются полиномиальными над $\mathbb{Z}_{2^m}$, обладает следующим свойством: если известны координаты неизвестных $x_1, \dots, x_n$ до i -го порядка включительно, то задача нахождения $(i+1)$ -х координат неизвестных сводится к решению системы линейных булевых уравнений. Следовательно, решение систем таких уравнений может быть осуществлено покоординатным способом. А именно, если найдены младшие координаты неизвестных (для чего может потребоваться решить систему нелинейных булевых уравнений), то определение остальных координат неизвестных осуществляется путем последовательного решения систем

линейных булевых уравнений. Такой метод решения систем полиномиальных уравнений в [2, 3] назван методом покоординатной линеаризации.

Класс функций, обладающих данным свойством, гораздо шире класса полиномиальных функций. В статье будет предложено два различных подхода к изучению таких функций. Первый из них конструктивный, а второй — в некотором смысле аксиоматический, основанный на формализации процесса покоординатного нахождения решений систем уравнений. Конструктивный подход фактически дает явный способ построения и задания подобных функций, а аксиоматический — описание всего их класса.

§ 1. Класс функций с вариационно-координатной полиномиальностью

1.1 Определение и общие свойства функций с вариационно-координатной полиномиальностью

Данный параграф целиком посвящен конструктивному подходу к определению функций, обладающих свойством покоординатной разрешимости составленных из них систем уравнений. Будет дано определение и будут изучены основные свойства класса функций, получивших в настоящей статье название «функции с вариационно-координатной полиномиальностью». Всюду далее предполагается, что m, n являются произвольными натуральными числами.

Определение 1. Для функции $f(x_1, \dots, x_n): \mathbb{Z}_{2^m}^n \rightarrow \mathbb{Z}_{2^m}$ и числа $j \in \{0, \dots, m-1\}$ отображение $\gamma_j f: \mathbb{Z}_{2^m}^n \rightarrow \mathcal{B}$, определяемое по правилу

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

для всех $\alpha \in \mathbb{Z}_{2^m}^n$, будем называть j -й координатной функцией функции f , или j -м координатным отображением.

Отметим, что любую координатную функцию $\gamma_j f$ можно рассматривать в то же время как булеву функцию $\gamma_j f: \mathcal{B}^{nm} \rightarrow \mathcal{B}$ от nm переменных, в роли которых выступают координаты $x_1^{(j)}, \dots, x_n^{(j)}$, $j = 0, \dots, m-1$. При этом всюду далее считаем, что порядок следования переменных такой функции идет в соответствии с ростом номеров координат, т.е. $\gamma_j f = \gamma_j f(x_1^{(0)}, \dots, x_n^{(0)}, \dots, x_1^{(m-1)}, \dots, x_n^{(m-1)})$.

Определение 2. Функцию $f(x_1, \dots, x_n): \mathbb{Z}_{2^m}^n \rightarrow \mathbb{Z}_{2^m}$ назовем *вариационно-координатно полиномиальной* (или *ВКП-функцией*), если для любого $j \in \{0, \dots, m-1\}$ существует полиномиальная функция $p_j(x_1, \dots, x_n)$

из $\mathbf{P}_{2^m}(n)$, j -я координатная функция которой совпадает с j -й координатной функцией $f(x_1, \dots, x_n)$, т. е.

$$\gamma_j f = \gamma_j p_j, \quad j = 0, \dots, m-1.$$

При этом в условиях определения 2 будем говорить, что функция $f(x_1, \dots, x_n)$ обладает свойством вариационно-координатной полиномиальности, а $p_j(x_1, \dots, x_n)$ является многочленом j -й координаты функции $f(x_1, \dots, x_n)$, или j -м координатным многочленом (отметим, что данный многочлен для функции $f(x_1, \dots, x_n)$ определяется неоднозначно). Использование при этом слова «вариационно-» подчеркивает тот факт, что данные координатные многочлены могут быть разными для различных координат, т. е. могут меняться от координаты к координате. Класс всех ВКП-функций от n переменных над $\mathbb{Z}_{2^m}$ обозначим через $\mathbf{CP}_{2^m}(n)$.

Утверждение 1. Для любой $f \in \mathbf{CP}_{2^m}(n)$, для любого $\alpha = (a_1, \dots, a_n) \in \mathbb{Z}_{2^m}^n$

$$\gamma_0 f(\alpha) \equiv p_0(\gamma_0(a_1), \dots, \gamma_0(a_n)) \pmod{2}. \quad (1)$$

Утверждение 2. Для любых $m, n \in \mathbb{N}$ имеет место включение

$$\mathbf{P}_{2^m}(n) \subseteq \mathbf{CP}_{2^m}(n).$$

Доказательство данного факта очевидно. Действительно, пусть $f(x_1, \dots, x_n) \in \mathbf{P}_{2^m}(n)$ и $p(x_1, \dots, x_n)$ — представляющий ее многочлен. Следовательно, $f(x_1, \dots, x_n)$ является ВКП-функцией, у которой $p_j(x_1, \dots, x_n) = p(x_1, \dots, x_n)$, $j = 0, \dots, m-1$. ■

Итак, любая полиномиальная функция является ВКП-функцией. Следовательно, возникает вопрос, является ли включение $\mathbf{P}_{2^m}(n)$ в $\mathbf{CP}_{2^m}(n)$ строгим. Оказывается (это будет показано в п. 1.3), что при $m \geq 3$ данное включение строгое, а при $m = 2$ рассматриваемые классы совпадают.

Прежде чем описывать дальнейшие свойства ВКП-функций, напомним некоторые определения [1].

Определение 3. 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 $i \in \{1, \dots, n\}$.

Определение 4. Функция $f(x_1, \dots, x_n): \mathbb{Z}_{2^m}^n \rightarrow \mathbb{Z}_{2^m}$ сохраняет отношение сравнимости по модулю $d \mid 2^m$, если на сравнимых по модулю d наборах она принимает сравнимые значения по модулю d .

Определение 5. Класс функций сохраняет отношение сравнимости по модулю $d \mid 2^m$, если любая функция из заданного класса сохраняет это отношение.

Обозначим через $\mathbf{D}_{2^m}(n)$ класс всех функций над $\mathbb{Z}_{2^m}$ от n переменных, сохраняющих отношение сравнимости по любому нетривиальному делителю 2^m . В этой связи упомянем работы В.С. Анашина [5, 6], в которых рассматривались функции, определенные на кольце целых p -адических чисел и сохраняющие отношение сравнимости, где также изучались их свойства.

Легко показать, используя простейшие свойства сравнений, что $\mathbf{P}_{2^m}(n) \subseteq \mathbf{D}_{2^m}(n)$. Следующая теорема, показывает, что ВКП-функции обладают тем же свойством.

Теорема 1. Для любых $m, n \in \mathbb{N}$ справедливо включение

$$\mathbf{CP}_{2^m}(n) \subseteq \mathbf{D}_{2^m}(n).$$

Доказательство. Пусть $f(x_1, \dots, x_n)$ — произвольная ВКП-функция из $\mathbf{CP}_{2^m}(n)$:

$$f(x_1, \dots, x_n) = (\gamma_0 p_0(x_1, \dots, x_n), \dots, \gamma_{m-1} p_{m-1}(x_1, \dots, x_n)),$$

$d = 2^l$ — произвольный делитель 2^m , $l \in \{1, \dots, m-1\}$ и $\alpha \equiv \beta \pmod{d}$. Так как $p_i(x_1, \dots, x_n)$, $i = 0, \dots, m-1$, — многочлены, то $p_i(\alpha) \equiv p_i(\beta) \pmod{d}$. Далее заметим, что

$$p_i(\alpha) = \sum_{j=0}^{m-1} 2^j \cdot \gamma_j p_i(\alpha) \equiv \sum_{j=0}^{l-1} 2^j \cdot \gamma_j p_i(\alpha) \pmod{d}.$$

А значит

$$p_i(\alpha) = \sum_{j=0}^{l-1} 2^j \cdot \gamma_j p_i(\alpha) \equiv \sum_{j=0}^{l-1} 2^j \cdot \gamma_j p_i(\beta) \equiv p_i(\beta) \pmod{d}.$$

Откуда получим, что $\gamma_j p_i(\alpha) = \gamma_j p_i(\beta)$ для всех $j \in \{0, \dots, l-1\}$, $i \in \{0, \dots, m-1\}$. В частности, $\gamma_j p_j(\alpha) = \gamma_j p_j(\beta)$ для всех $j \in \{0, \dots, l-1\}$.

Имеем

$$\begin{aligned} f(\alpha) &= \sum_{j=0}^{m-1} 2^j \cdot \gamma_j p_j(\alpha) \equiv \sum_{j=0}^{l-1} 2^j \cdot \gamma_j p_j(\alpha) \pmod{d} = \sum_{j=0}^{l-1} 2^j \cdot \gamma_j p_j(\beta) \equiv \\ &\equiv \sum_{j=0}^{m-1} 2^j \cdot \gamma_j p_j(\beta) \pmod{d} = f(\beta). \blacksquare \end{aligned}$$

Таким образом, класс функций с вариационно-координатной полиномиальностью так же, как и класс полиномиальных функций, сохраняет отношение сравнимости по любому нетривиальному делителю 2^m .

Следующее утверждение играет базовую роль при решении систем уравнений, составленных из ВКП-функций.

Утверждение 3. Пусть $f \in \mathbf{CP}_{2^m}(n)$, $m > 1$, $n \in \mathbb{N}$. Тогда для любого $j \in \{1, \dots, m-1\}$ координатная функция $\gamma_j f: \mathcal{B}^{nm} \rightarrow \mathcal{B}$:

1. является булевой функцией от координат переменных порядков, не больших j ;
2. является аффинной функцией по координатам $x_1^{(j)}, \dots, x_n^{(j)}$ при любых фиксированных координатах меньшего порядка $x_i^{(k)}$, $1 \leq i \leq n$, $0 \leq k < j$, т. е. существуют такие $a_j, a_{j1}, \dots, a_{jn} \in \mathcal{B}$, зависящие от указанных координат что

$$\gamma_j f(x_1, \dots, x_n) = a_{j1} \cdot x^{(j)} \oplus \dots \oplus a_{jn} \cdot x_n^{(j)} \oplus a_j.$$

Доказательство. 1. В доказательстве теоремы 1 было показано, что если $\alpha \equiv \beta \pmod{2^{j+1}}$, где $\alpha, \beta \in \mathbb{Z}_{2^m}^n$, $j \in \{1, \dots, m-2\}$, то $\gamma_j p(\alpha) = \gamma_j p(\beta)$ для любой полиномиальной функции $p(x_1, \dots, x_n) \in \mathbf{P}_{2^m}(n)$. Поэтому для произвольных ВКП-функции $f \in \mathbf{CP}_{2^m}(n)$ и $j \in \{1, \dots, m-2\}$ (очевидно, при $j = m-1$ утверждение верно) имеет место следующее:

$$\begin{aligned} \gamma_j f(x_1, \dots, x_n) &= \gamma_j p_j(x_1, \dots, x_n) = \gamma_j p_j(x_1 \bmod 2^{j+1}, \dots, x_n \bmod 2^{j+1}) = \\ &= \gamma_j p_j \left(\sum_{i=0}^j 2^i \cdot x_1^{(i)}, \dots, \sum_{i=0}^j 2^i \cdot x_n^{(i)} \right). \end{aligned}$$

А поскольку функцию $\gamma_j f$ можно рассматривать как булеву от координат входящих в нее переменных, то, как видно из приведенного выше выражения существенно зависеть она будет только от тех координат, порядок которых не больше j .

2. Пусть $f \in \mathbf{CP}_{2^m}(n)$ и $j \in \{1, \dots, m-1\}$. Рассмотрим ее многочлен j -й координаты $p_j(x_1, \dots, x_n)$:

$$p_j(x_1, \dots, x_n) = \sum_{k=0}^n \sum_{i_1, \dots, i_k} b_{i_1 \dots i_k} x_{i_1} \dots x_{i_k}.$$

Справедливо равенство

$$\gamma_j p_j(x_1, \dots, x_n) = \gamma_j(p_j(x_1, \dots, x_n) \bmod 2^{j+1}). \quad (2)$$

Зафиксируем произвольным образом координаты $x_1^{(i)}, \dots, x_n^{(i)}$, $i = 0, \dots, j-1$. Тогда согласно пункту 1 и равенству выше, имеем:

$$\begin{aligned} \gamma_j p_j(x_1, \dots, x_n) &= \gamma_j \left(p_j \left(\sum_{i=0}^j 2^i \cdot x_1^{(i)}, \dots, \sum_{i=0}^j 2^i \cdot x_n^{(i)} \right) \bmod 2^{j+1} \right) = \\ &= \gamma_j \left(\sum_{k=0}^n \sum_{i_1, \dots, i_k} b_{i_1 \dots i_k} \left(\sum_{i=0}^j 2^i \cdot x_{i_1}^{(i)} \right) \dots \left(\sum_{i=0}^j 2^i \cdot x_{i_k}^{(i)} \right) \bmod 2^{j+1} \right). \end{aligned} \quad (3)$$

Раскрывая скобки, получим:

$$\begin{aligned} \gamma_j p_j(x_1, \dots, x_n) &= \\ &= \gamma_j \left(\dots + 2^j \cdot (a_{j1} \cdot x_1^{(j)} + \dots + a_{jn} \cdot x_n^{(j)} + a_j) \bmod 2^{j+1} \right), \end{aligned}$$

где аргументом γ_j является выражение, получаемое приведением подобных членов по степеням двойки и $x_i^{(k)}$ после перемножения; a_{ji} — полученные таким образом числа, не зависящие от j -х координат. Заметим, что здесь отсутствуют слагаемые вида $2^j x_l^{(j)} \cdot x_q^{(j)}$, поскольку они могли получиться только в результате умножения $2^j x_l^{(j)}$ на $2^j x_q^{(j)}$, но их произведение по модулю 2^{j+1} очевидно, равно нулю.

Поэтому

$$\gamma_j p_j(x_1, \dots, x_n) = a_{j1} \cdot x_1^{(j)} \oplus \dots \oplus a_{jn} \cdot x_n^{(j)} \oplus a_j,$$

а значит, функция $\gamma_j p_j(x_1, \dots, x_n)$ является аффинной по $x_1^{(j)}, \dots, x_n^{(j)}$. ■

Следствие. Если $f \in \mathbf{CP}_{2^m}(n)$, $m > 1$, то для любого $j \in \{1, \dots, m-1\}$ существуют булевы функции $g_j: \mathcal{B}^{jn} \rightarrow \mathcal{B}$, $g_{ji}: \mathcal{B}^n \rightarrow \mathcal{B}$, $i = 1, \dots, n$, для которых выполнено равенство

$$\begin{aligned} \gamma_j f(x_1, \dots, x_n) = & \bigoplus_{i=1}^n g_{ji}(x_1^{(0)}, \dots, x_n^{(0)}) \cdot x_i^{(j)} \oplus \\ & \bigoplus g_j(x_1^{(0)}, \dots, x_n^{(0)}, \dots, x_1^{(j-1)}, \dots, x_n^{(j-1)}). \end{aligned} \quad (4)$$

Действительно, согласно доказанному при любых фиксированных $x_1^{(0)}, \dots, x_n^{(0)}, \dots, x_1^{(j-1)}, \dots, x_n^{(j-1)}$, координатная функция $\gamma_j f(x_1, \dots, x_n)$ является аффинной по $x_1^{(j)}, \dots, x_n^{(j)}$, т. е. существуют такие

$$\begin{aligned} a_j &= g_j(x_1^{(0)}, \dots, x_n^{(0)}, \dots, x_1^{(j-1)}, \dots, x_n^{(j-1)}), \\ a_{ji} &= g_{ji}(x_1^{(0)}, \dots, x_n^{(0)}, \dots, x_1^{(j-1)}, \dots, x_n^{(j-1)}), \quad i = 1, \dots, n, \end{aligned}$$

что

$$\begin{aligned} \gamma_j f(x_1, \dots, x_n) = & \bigoplus_{i=1}^n g_{ji}(x_1^{(0)}, \dots, x_n^{(0)}, \dots, x_1^{(j-1)}, \dots, x_n^{(j-1)}) \cdot x_i^{(j)} \oplus \\ & \bigoplus g_j(x_1^{(0)}, \dots, x_n^{(0)}, \dots, x_1^{(j-1)}, \dots, x_n^{(j-1)}). \end{aligned}$$

Осталось показать, что булевы функции $g_{ji}(x_1^{(0)}, \dots, x_n^{(0)}, \dots, x_1^{(j-1)}, \dots, x_n^{(j-1)})$ не зависят от переменных $x_1^{(1)}, \dots, x_n^{(1)}, \dots, x_1^{(j-1)}, \dots, x_n^{(j-1)}$. Но это очевидно следует из равенства (3), поскольку получить коэффициент при $x_i^{(j)}$ можно лишь умножением $2^j x_i^{(j)}$ на $x_i^{(0)}$, иначе произведение $2^j x_i^{(j)}$ и $2^k x_i^{(k)}$ (при $k \in \{1, \dots, j-1\}$) равно нулю по модулю 2^{j+1} . А значит, выражение g_{ji} при $x_i^{(j)}$ не зависит от $x_1^{(k)}, \dots, x_n^{(k)}$, где $k = 1, \dots, j-1$. ■

Приведенное утверждение и следствие из него описывают свойство ВКП-функций, играющее важную роль при решении составленных из этих функций систем уравнений (в дальнейшем такие системы будем называть системами ВКП-уравнений). Идея использования данного свойства заключается в следующем. После нахождения координат неизвестных до j -го порядка включительно, $(j+1)$ -я координатная функция каждой из ВКП-функций, входящих в систему, становится аффинной относительно $(j+1)$ -х координат неизвестных, а значит можно свести задачу их нахождения к решению некоторой системы линейных уравнений.

Укажем одно простое свойство ВКП-функций, которое представляет особый интерес: суперпозиция ВКП-функций с полиномиальными дает снова ВКП-функцию.

Утверждение 4. Для любых $m, n, k \in \mathbb{N}$ класс $\mathbf{CP}_{2^m}(n)$ замкнут относительно суперпозиции с полиномиальными функциями из $\mathbf{P}_{2^m}(k)$ в том смысле, что $f(g_1, \dots, g_n) \in \mathbf{CP}_{2^m}(k)$ для любой $f \in \mathbf{CP}_{2^m}(n)$ и любых полиномиальных функций $g_1, \dots, g_n \in \mathbf{P}_{2^m}(k)$.

Действительно, суперпозиция полиномиальных функций есть снова полиномиальная, и при этом каждая j -я координатная функция $f(g_1, \dots, g_n)$ совпадает с j -й координатной функцией $p_j(g_1, \dots, g_n)$, где $p_j(x_1, \dots, x_n)$ — многочлен j -й координаты $f(x_1, \dots, x_n)$. ■

1.2 Оценка числа ВКП функций от n переменных над $\mathbb{Z}_{2^m}$

Поскольку каждая ВКП-функция однозначно определяется соответствующими координатными отображениями полиномиальных функций, постольку мощность множества ВКП-функций равна произведению мощностей множества таких отображений. При $j = 0$ количество различных координатных отображений $\gamma_0 p(x_1, \dots, x_n)$ (где $p(x_1, \dots, x_n) \in \mathbf{P}_{2^m}(n)$) равно числу булевых функций от n переменных (см. утверждение 1) и равно 2^{2^n} . Для каждого $j \in \{1, \dots, m-1\}$ оценим сверху количество различных функций $\gamma_j p(x_1, \dots, x_n)$ (где $p(x_1, \dots, x_n) \in \mathbf{P}_{2^m}(n)$), что даст верхнюю оценку мощности класса $\mathbf{CP}_{2^m}(n)$.

Договоримся далее для простоты записи обозначать векторы переменных $(x_1, \dots, x_n)$ жирными буквами, например $\mathbf{x}$, и функцию $f(x_1, \dots, x_n)$ записывать кратко $f(\mathbf{x})$. Обозначим через $\mathcal{B}^n = \{\theta = (h_1, \dots, h_n) \in \mathbb{Z}_{2^m}^n : h_i \in \mathcal{B}, i = 1, \dots, n\}$ множество векторов из $\mathbb{Z}_{2^m}^n$, у которых каждая компонента равна либо 0, либо 1 ($\mathcal{B}^n$ есть «единичный подкуб» множества $\mathbb{Z}_{2^m}^n$).

Лемма 1 ([3]). Для любого многочлена $p(\mathbf{x}) \in \mathbb{Z}_{2^m}[x_1, \dots, x_n]$ и любых $j \in \{1, \dots, m-1\}$, $\theta = (h_1, \dots, h_n) \in \mathcal{B}^n$ справедливо сравнение

$$p(\mathbf{x} + 2^j \cdot \theta) \equiv p(\mathbf{x}) + 2^j \sum_{i=1}^n p'_{x_i}(\mathbf{x}) \cdot h_i \pmod{2^{j+1}}, \quad (5)$$

где $p'_{x_i}(\mathbf{x})$ — формальная частная производная многочлена $p(\mathbf{x})$ по переменной x_i .

Лемма 2. Если $a = x + 2^j y$, где $x, y \in \mathbb{Z}_{2^m}$ и $j \in \{0, \dots, m-1\}$, то

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

Доказательство. Легко видеть, что

$$\begin{aligned}\gamma_j(a) &= \gamma_j(x + 2^j y) = \gamma_j(x + 2^j(\gamma_0(y) + 2 \cdot \gamma_1(y) + \dots + 2^{m-1} \gamma_{m-1}(y))) = \\ &= \gamma_j(x) \oplus \gamma_0(y). \blacksquare\end{aligned}$$

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

$$\gamma_j p(\mathbf{x} + 2^j \cdot \theta) = \gamma_j p(\mathbf{x}) \oplus \gamma_0 \left(\sum_{i=1}^n p'_{x_i}(\mathbf{x}) \cdot h_i \right). \quad (6)$$

Рассмотрим выражение $\gamma_0 \left(\sum_{i=1}^n p'_{x_i}(\mathbf{x}) \cdot h_i \right)$, стоящее в правой части (6). Согласно утверждению 1

$$\gamma_0 \left(\sum_{i=1}^n p'_{x_i}(\mathbf{x}) \cdot h_i \right) \equiv \sum_{i=1}^n p'_{x_i}(\mathbf{x}) \cdot h_i \pmod{2}.$$

Сумма $\sum_{i=1}^n p'_{x_i}(\mathbf{x}) \cdot h_i$ есть многочлен, а значит

$$\sum_{i=1}^n p'_{x_i}(\mathbf{x}) \cdot h_i \equiv \sum_{i=1}^n p'_{x_i}(\mathbf{x}^{(0)}) \cdot h_i \pmod{2},$$

где $\mathbf{x}^{(0)} = (x_1^{(0)}, \dots, x_n^{(0)})$. Тогда равенство (6) можно переписать следующим образом:

$$\gamma_j p(\mathbf{x} + 2^j \cdot \theta) \equiv \gamma_j p(\mathbf{x}) \oplus \sum_{i=1}^n p'_{x_i}(\mathbf{x}) \cdot h_i \pmod{2}. \quad (7)$$

Обозначим через $\theta_i = (\delta_{i,1}, \dots, \delta_{i,n}) \in \mathcal{B}^n$, $i \in \{1, \dots, n\}$, где $\delta_{i,j}$ — символ Кронекера. Используя полученное выше сравнение при $\theta = \theta_i$ и $\mathbf{x} = \mathbf{x}^{(0)}$, придем к сравнению

$$p'_{x_i}(\mathbf{x}^{(0)}) \equiv \gamma_j p(\mathbf{x}^{(0)} + 2^j \cdot \theta_i) \oplus \gamma_j p(\mathbf{x}^{(0)}) \pmod{2}.$$

Подстановка его в (7) доказывает следующую теорему.

Теорема 2. Для любого многочлена $p(\mathbf{x}) \in \mathbb{Z}_{2^m}[x_1, \dots, x_n]$ и любых $j \in \{1, \dots, m-1\}$, $\theta = (h_1, \dots, h_n) \in \mathcal{B}^n$ справедливо равенство

$$\gamma_j p(\mathbf{x} + 2^j \cdot \theta) = \gamma_j p(\mathbf{x}) \oplus \sum_{i=1}^n \left(\gamma_j p(\mathbf{x}^{(0)} + 2^j \cdot \theta_i) \oplus \gamma_j p(\mathbf{x}^{(0)}) \right) \cdot h_i, \quad (8)$$

где $\mathbf{x}^{(0)} = (x_1^{(0)}, \dots, x_n^{(0)})$ и $\theta_i = (\delta_{i,1}, \dots, \delta_{i,n})$, $i = 1, \dots, n$.

Утверждение 5. Если функция $p(\mathbf{x}) \in \mathbf{P}_{2^m}(n)$, то ее j -я координатная функция $\gamma_j p: \mathcal{B}^{nm} \rightarrow \mathcal{B}$, $j \in \{1, \dots, m-1\}$, однозначно определяется по значениям на множестве $\{0, \dots, 2^j - 1\}^n$ и значениям $\gamma_j p(\theta + 2^j \cdot \theta_i)$, $\theta \in \mathcal{B}^n$, $i = 1, \dots, n$.

Доказательство. Пусть $\alpha = (a_1, \dots, a_n) \in \mathbb{Z}_{2^m}^n$. Покажем, как по указанным в условии величинам вычислить $\gamma_j p(\alpha)$. Разделим каждое a_k на 2^j , $k = 1, \dots, n$, с остатком и представим вектор α в виде

$$\alpha = \beta + 2^j \cdot \nu,$$

где $\beta = (b_1, \dots, b_n) \in \{0, \dots, 2^j - 1\}^n$. Аналогично, разделим каждое полученное b_k на 2, $k = 1, \dots, n$, с остатком и представим ν в виде:

$$\nu = \theta + 2 \cdot \nu_1,$$

где $\theta = (h_1, \dots, h_n) \in \mathcal{B}^n$. Имеем

$$\alpha = \beta + 2^j \cdot \nu = \beta + 2^j \cdot (\theta + 2 \cdot \nu_1) = \beta + 2^j \cdot \theta + 2^{j+1} \cdot \nu_1.$$

Поскольку

$$\gamma_j p(\alpha) = \gamma_j p(\beta + 2^j \cdot \theta + 2^{j+1} \cdot \nu_1) = \gamma_j p(\beta + 2^j \cdot \theta),$$

то по теореме 2

$$\gamma_j p(\alpha) = \gamma_j p(\beta + 2^j \cdot \theta) = \gamma_j p(\beta) \oplus \sum_{i=1}^n \left(\gamma_j p(\beta^{(0)} + 2^j \cdot \theta_i) \oplus \gamma_j p(\beta^{(0)}) \right) \cdot h_i,$$

где $\beta^{(0)} = (b_1^{(0)}, \dots, b_n^{(0)}) \in \mathcal{B}^n$. При этом по условию утверждения известны значения $\gamma_j p(\beta)$, $\gamma_j p(\beta^{(0)})$ и $\gamma_j p(\beta^{(0)} + 2^j \cdot \theta_i)$, а значит, по ним находится $\gamma_j p(\alpha)$. ■

Согласно доказанному утверждению j -е координатное отображение ($j \in \{1, \dots, m-1\}$) любой полиномиальной функции однозначно определяется по значениям на множестве $\{0, \dots, 2^j - 1\}^n$ и векторах вида $\theta + 2^j \cdot \theta_i$, $\theta \in \mathcal{B}^n$, $i = 1, \dots, n$. Количество таких значений равно $2^{jn} + n \cdot 2^n$. А значит, число всех различных j -х координатных отображений полиномиальных функций от n переменных над $\mathbb{Z}_{2^m}$ не превосходит $2^{2^{jn} + n \cdot 2^n}$. Напомним, что количество ВКП-функций равно произведению соответствующих мощностей различных координатных отображений. Отсюда получим оценку мощности класса $\mathbf{CP}_{2^m}(n)$.

Утверждение 6. Для любых $m, n \in \mathbb{N}$ верна оценка мощности множества ВКП-функций от n переменных над $\mathbb{Z}_{2^m}$:

$$|\mathbf{CP}_{2^m}(n)| \leq 2^{2^n + (m-1)n \cdot 2^n + \frac{2^n(2^n(m-1)-1)}{2^n-1}}. \quad (9)$$

Доказательство. Согласно приведенным рассуждениям имеем

$$\begin{aligned} |\mathbf{CP}_{2^m}(n)| &\leq 2^{2^n} \prod_{j=1}^{m-1} 2^{2^{jn} + n \cdot 2^n} = 2^{2^n} \cdot 2^{\sum_{j=1}^{m-1} (2^{jn} + n \cdot 2^n)} = \\ &= 2^{2^n + (m-1)n \cdot 2^n + \frac{2^n(2^n(m-1)-1)}{2^n-1}}. \blacksquare \end{aligned}$$

1.3 Соотношение между классами полиномиальных и ВКП-функций над $\mathbb{Z}_{2^m}$

Вернемся к вопросу о соотношении между классами функций $\mathbf{P}_{2^m}(n)$ и $\mathbf{CP}_{2^m}(n)$ при $m > 1$ (если $m = 1$, то их совпадение очевидно).

Утверждение 7. Для любого $n \in \mathbb{N}$ справедливо равенство

$$|\mathbf{P}_4(n)| = 2^{2^n(n+2)}.$$

Доказательство утверждения несложно получить, используя результаты, изложенные в [4].

Теорема 3. Для любого $n \in \mathbb{N}$ классы полиномиальных и ВКП-функций над $\mathbb{Z}_4$ от n переменных совпадают: $\mathbf{P}_4(n) = \mathbf{CP}_4(n)$.

Доказательство. Согласно утверждению 7

$$|\mathbf{P}_4(n)| = 2^{2^n(n+2)}.$$

С другой стороны, согласно неравенству (8)

$$|\mathbf{CP}_4(n)| \leq 2^{2^n + n2^n + 2^n} = 2^{2^n(n+2)}.$$

А значит, $|\mathbf{CP}_4(n)| \leq |\mathbf{P}_4(n)|$. Но при этом $\mathbf{P}_4(n) \subseteq \mathbf{CP}_4(n)$. Следовательно, имеет место равенство $\mathbf{P}_4(n) = \mathbf{CP}_4(n)$. $\blacksquare$

Покажем далее, что при всех $m \geq 3$, $n \in \mathbb{N}$ классы $\mathbf{P}_{2^m}(n)$ и $\mathbf{CP}_{2^m}(n)$ не совпадают. Введем несколько обозначений и сформулируем необходимые леммы.

Пусть $(x)_j = x(x-1)\dots(x-j+1)$ при $j \geq 1$ и $(x)_0 = 1$; обозначим через $\mathbf{O}_{2^m}$ идеал кольца $\mathbb{Z}_{2^m}[x_1, \dots, x_n]$, состоящий из многочленов, задающих тождественно равные нулю функции:

$$\mathbf{O}_{2^m} = \{f(x_1, \dots, x_n) \in \mathbb{Z}_{2^m}[x_1, \dots, x_n] : f(\alpha) = 0 \text{ для любого } \alpha \in \mathbb{Z}_{2^m}^n\}.$$

Обозначим через $s(2^m)$ минимальное число $i \in \{0, \dots, 2^m - 1\}$, для которого $(x)_i \in \mathbf{O}_{2^m}$.

Доказательства приведенных ниже лемм 3–5 приведены в [4].

Лемма 3. Число $s(2^m)$ равно такому $i \in \{0, \dots, 2^m - 1\}$, что

$$\begin{aligned} i! &\equiv 0 \pmod{2^m}, \\ (i-1)! &\equiv 0 \pmod{2^m}. \end{aligned}$$

Лемма 4. Число $s(2^m)$ равно минимальному натуральному N , для которого

$$\left\lfloor \frac{N}{2} \right\rfloor + \left\lfloor \frac{N}{2^2} \right\rfloor + \dots + \left\lfloor \frac{N}{2^{m-1}} \right\rfloor \geq m.$$

Пользуясь леммой 4, можно получить значения $s(2^m)$, приведенные в таблице 1.

Таблица 1

2^m	2	4	8	16	32	64	128	256	512
$s(2^m)$	2	4	4	6	8	8	8	10	12

Лемма 5. Любая функция $f(x_1, \dots, x_n) \in \mathbf{P}_{2^m}(n)$ однозначно определяется своими значениями на векторах $\alpha = (a_1, \dots, a_n) \in \mathbb{Z}_{2^m}^n$, где $0 \leq a_i \leq s(2^m) - 1$, $i = 1, \dots, n$.

Утверждение 8. Для любого $n \in \mathbb{N}$ классы полиномиальных и ВКП-функций над $\mathbb{Z}_8$ от n переменных не совпадают, т. е. $\mathbf{P}_8(n) \neq \mathbf{CP}_8(n)$.

Доказательство. Докажем утверждение сначала при $n = 1$. Для этого укажем такую ВКП-функцию из $\mathbf{CP}_8(1)$, которая не является полиномиальной, т. е. не лежит в классе $\mathbf{P}_8(1)$.

Заметим, что значение $s(8) = 4$ (см. табл. 1), поэтому в силу леммы 5 любая полиномиальная функция от одной переменной над $\mathbb{Z}_8$ однозначно определяется по значениям на множестве $\{0, 1, 2, 3\}$.

Рассмотрим ВКП-функцию $f(x) \in \mathbf{CP}_8(1)$, имеющую следующие координатные многочлены:

$$\begin{cases} p_0(x) = x + 1, \\ p_1(x) = x, \\ p_2(x) = 6x + 3. \end{cases}$$

Значения этой функции приведены в таблице 2.

Таблица 2

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

Многочлен $3x^4 + 2x^3 + x^2 + x + 1$ задает полиномиальную функцию $g(x)$, значения которой представлены в таблице 3.

Таблица 3

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

Как видно из таблиц 2 и 3, значения функций $f(x)$ и $g(x)$ совпадают на множестве $\{0, \dots, 3\} = \{0, \dots, s(8) - 1\}$ и не совпадают на множестве $\{4, \dots, 7\}$. Следовательно, $f(x)$ не является полиномиальной, иначе получим противоречие с однозначной определенностью $g(x)$ по значениям на множестве $\{0, \dots, 3\}$. При $n = 1$ утверждение доказано.

Пусть теперь $n \in \mathbb{N}$, $n \geq 2$. Покажем, что $\mathbf{P}_8(n) \neq \mathbf{CP}_8(n)$. Достаточно рассмотреть функцию $q(x_1, \dots, x_n) \in \mathbf{CP}_8(n)$, у которой координатные многочлены имеют вид

$$\begin{cases} p_0(x_1, \dots, x_n) = x_1 + 1, \\ p_1(x_1, \dots, x_n) = x_1, \\ p_2(x_1, \dots, x_n) = 6x_1 + 3. \end{cases}$$

Если предположить, что она является полиномиальной, то она будет таковой и по переменной x_1 , т. е. при любых фиксированных $a_2, \dots, a_n \in \mathbb{Z}_8$ функция $h(x) = q(x, a_2, \dots, a_n)$ должна лежать в классе $\mathbf{P}_8(1)$. Получено противоречие, поскольку $h(x)$ совпадает с приведенной выше функцией $f(x)$, которая, как было доказано, не лежит в $\mathbf{P}_8(1)$. ■

Чтобы показать несовпадение рассматриваемых классов уже при любом $m \geq 3$, нам потребуется ввести следующую конструкцию. Пусть $m \in \mathbb{N}$ и $\tau: (\mathbb{Z}_{2^{m+1}}, +) \rightarrow (\mathbb{Z}_{2^m}, +)$ — отображение, задаваемое по правилу

$$\tau(a) = a \bmod 2^m, \quad a \in \mathbb{Z}_{2^{m+1}}.$$

Тогда τ является эпиморфизмом абелевых групп и его можно продолжить до эпиморфизма $\tau^*: (\mathbb{Z}_{2^{m+1}}^n, +) \rightarrow (\mathbb{Z}_{2^m}^n, +)$:

$$\tau^*(\alpha) = (\tau(a_1), \dots, \tau(a_n)), \quad \alpha = (a_1, \dots, a_n) \in \mathbb{Z}_{2^{m+1}}^n.$$

Определение 6. Функция $f: \mathbb{Z}_{2^{m+1}}^n \rightarrow \mathbb{Z}_{2^{m+1}}$ является *приводимой по модулю 2^m* , если существует такая функция $\hat{f}: \mathbb{Z}_{2^m}^n \rightarrow \mathbb{Z}_{2^m}$, что для любого $\alpha \in \mathbb{Z}_{2^{m+1}}^n$ выполнено равенство

$$\hat{f}(\tau^*(\alpha)) = \tau(f(\alpha)). \quad (10)$$

Сформулируем следующий очевидный критерий приводимости функции по модулю 2^m .

Утверждение 9. Функция $f: \mathbb{Z}_{2^{m+1}}^n \rightarrow \mathbb{Z}_{2^{m+1}}$ является *приводимой по модулю 2^m* тогда и только тогда, когда она сохраняет отношение сравнимости данному модулю.

Согласно критерию любые функции, сохраняющие отношение сравнимости по модулю 2^m приводимы. А следовательно, приводимыми являются все полиномиальные и ВКП-функции над $\mathbb{Z}_{2^{m+1}}$. Для класса K приводимых по модулю 2^m функций будем обозначать через $\hat{K}$ класс, полученный приведением по модулю 2^m каждой функции $f \in K$.

Утверждение 10. Для любых $m, n \in \mathbb{N}$ справедливо равенство

$$\widehat{\mathbf{P}_{2^{m+1}}}(n) = \mathbf{P}_{2^m}(n). \quad (11)$$

Утверждение 11. Для любых $m, n \in \mathbb{N}$ справедливо равенство

$$\widehat{\mathbf{CP}_{2^{m+1}}}(n) = \mathbf{CP}_{2^m}(n). \quad (12)$$

Доказательство. Докажем равенство двух классов, показав их взаимное включение. Пусть $f \in \mathbf{CP}_{2^{m+1}}(n)$; тогда существуют такие полиномиальные функции $p_0, \dots, p_m \in \mathbf{P}_{2^{m+1}}(n)$, что

$$f(\alpha) = \sum_{j=0}^m 2^j \cdot \gamma_j p_j(\alpha), \quad \alpha \in \mathbb{Z}_{2^{m+1}}^n.$$

Отметим очевидные равенства

$$\gamma_j p_j(\alpha) = \gamma_j(p_j(\alpha) \bmod 2^m) = \gamma_j(\tau(p_j(\alpha))), \quad j \in \{0, \dots, m-1\}.$$

Рассмотрим ВКП-функцию $g \in \mathbf{CP}_{2^m}(n)$, имеющую координатные многочлены $\hat{p}_0, \dots, \hat{p}_{m-1} \in \mathbf{P}_{2^m}(n)$. Тогда для любого $\beta \in \mathbb{Z}_{2^m}^n$

$$g(\beta) = \sum_{j=0}^{m-1} 2^j \cdot \gamma_j \hat{p}_j(\beta).$$

Докажем, что $\hat{f} = g$. Для этого проверим выполнение (10). Пусть $\alpha \in \mathbb{Z}_{2^{m+1}}^n$ и $\beta = \tau^*(\alpha) \in \mathbb{Z}_{2^m}^n$. Имеем:

$$\begin{aligned} \tau(\hat{f}(\alpha)) &= \tau\left(\sum_{j=0}^m 2^j \cdot \gamma_j p_j(\alpha)\right) = \sum_{j=0}^{m-1} 2^j \cdot \gamma_j p_j(\alpha) = \\ &= \sum_{j=0}^{m-1} 2^j \cdot \gamma_j(p_j(\alpha) \bmod 2^m) = \\ &= \sum_{j=0}^{m-1} 2^j \cdot \gamma_j(\tau(p_j(\alpha))) = \sum_{j=0}^{m-1} 2^j \cdot \gamma_j \hat{p}_j(\beta) = g(\beta) = g(\tau^*(\alpha)). \end{aligned}$$

Таким образом, $\hat{f} \in \mathbf{CP}_{2^m}(n)$ и, следовательно, $\widehat{\mathbf{CP}_{2^{m+1}}(n)} \subseteq \mathbf{CP}_{2^m}(n)$.

Обратно, рассмотрим функцию $g \in \mathbf{CP}_{2^m}(n)$; пусть $q_0, \dots, q_{m-1}$ — ее координатные многочлены. Построим такую $\hat{f} \in \mathbf{CP}_{2^{m+1}}(n)$, что $\hat{f} = g$. Пусть $p_j \in \mathbf{P}_{2^{m+1}}(n)$, $j = 0, \dots, m-1$, — такие полиномиальные функции, что $\hat{p}_j = q_j$, и $p_m \in \mathbf{P}_{2^{m+1}}(n)$ произвольна. Положим

$$\hat{f}(\alpha) = \sum_{j=0}^m 2^j \cdot \gamma_j p_j(\alpha), \quad \alpha \in \mathbb{Z}_{2^{m+1}}^n.$$

Тогда, используя рассуждения, аналогичные приведенным выше, устанавливаем, что $\hat{f} = g$. А значит, $\mathbf{CP}_{2^m}(n) \subseteq \widehat{\mathbf{CP}_{2^{m+1}}(n)}$, и утверждение доказано. ■

Докажем теорему о соотношении классов полиномиальных и ВКП-функций при $m \geq 3$.

Теорема 4. Для любых $n \in \mathbb{N}$ и $m \geq 3$ класс ВКП-функций $\mathbf{CP}_{2^m}(n)$ не совпадает с классом полиномиальных $\mathbf{P}_{2^m}(n)$.

Докажем теорему методом полной математической индукции по $m \geq 3$ при произвольном фиксированном $n \in \mathbb{N}$. База индукции — утверждение 8. Пусть теорема верна при любом $m \leq k$, рассмотрим $m = k + 1$. Предположим противное: $\mathbf{CP}_{2^{k+1}}(n) = \mathbf{P}_{2^{k+1}}(n)$. Тогда согласно (11) и (12) верны равенства $\widehat{\mathbf{P}_{2^{k+1}}(n)} = \mathbf{P}_{2^k}(n)$ и $\widehat{\mathbf{CP}_{2^{k+1}}(n)} = \mathbf{CP}_{2^k}(n)$, а значит $\mathbf{CP}_{2^k}(n) = \mathbf{P}_{2^k}(n)$ и получаем противоречие с предположением индукции. ■

§ 2. Класс функций с координатной $\mathcal{L}$ -линейной разрешимостью ($\mathcal{L} \subseteq \{0, \dots, m - 1\}$)

Рассмотренное в предыдущем параграфе описание класса функций имеет конструктивный характер, поскольку в явном виде предлагает задание функций из этого класса. Важное свойство этих функций описывается в утверждении 3 и следствии из него: каждая j -я координатная функция ($j \geq 1$) ВКП-функции является аффинной по j -м координатам переменных (при фиксированных координатах меньшего порядка). Как отмечалось ранее, указанное свойство является ключевым при решении систем уравнений. Поэтому интересным представляется вопрос об описании всех функций над $\mathbb{Z}_{2^m}$, которые им обладают, поскольку системы уравнений, левые части которых образованы такими функциями, могут быть решены «покоординатно». В данном параграфе будет предложен в некотором смысле аксиоматический подход к определению функций с этим свойством.

Определение 7. Пусть $\mathcal{L} \subseteq \{0, \dots, m - 1\}$. Функцию $f(x_1, \dots, x_n): \mathbb{Z}_{2^m}^n \rightarrow \mathbb{Z}_{2^m}$ назовем координатно $\mathcal{L}$ -линейно разрешимой (или $\mathcal{L}$ -КЛР-функцией), если:

- 1) при всех $j \in \{0, \dots, m - 1\} \setminus \mathcal{L}$ ее j -я координатная функция $\gamma_j f$ существенно зависит от координат переменных $x_1^{(i)}, \dots, x_n^{(i)}$ порядков не превосходящих j ;
- 2) при всех $j \in \mathcal{L}$ ее j -я координатная функция $\gamma_j f$ существенно зависит от координат переменных $x_1^{(i)}, \dots, x_n^{(i)}$ порядков не превосходящих j и при этом является аффинной относительно j -х координат переменных $x_1^{(j)}, \dots, x_n^{(j)}$.

Другими словами, существуют такие булевы функции $g_{ji}, g_j: \mathcal{B}^{n_j} \rightarrow \mathcal{B}$, $j \in \mathcal{L}$, $i = 1, \dots, n$, и функции $g_j: \mathcal{B}^{n(j+1)} \rightarrow \mathcal{B}$, $j \in \{0, \dots, m - 1\} \setminus \mathcal{L}$, что

1) при всех $j \in \{0, \dots, m-1\} \setminus \mathcal{L}$

$$\gamma_j f(x_1, \dots, x_n) = g_j(x_1^{(0)}, \dots, x_n^{(0)}, \dots, x_1^{(j)}, \dots, x_n^{(j)}),$$

2) для любого $j \in \mathcal{L}$

$$\begin{aligned} \gamma_j f(x_1, \dots, x_n) = \\ = \oplus \sum_{i=1}^n g_{ji}(x_1^{(0)}, \dots, x_n^{(0)}, \dots, x_1^{(j-1)}, \dots, x_n^{(j-1)}) \cdot x_i^{(j)} \oplus \\ \oplus g_j(x_1^{(0)}, \dots, x_n^{(0)}, \dots, x_1^{(j-1)}, \dots, x_n^{(j-1)}). \end{aligned}$$

При заданном подмножестве $\mathcal{L} \subseteq \{0, \dots, m-1\}$ обозначим класс всех $\mathcal{L}$ -КЛР-функций от n переменных над $\mathbb{Z}_{2^m}$ через $\mathbf{CLS}_{2^m}^{\mathcal{L}}(n)$; в условиях определения 7 будем также говорить, что функция $f(x_1, \dots, x_n)$ обладает свойством координатной $\mathcal{L}$ -линейной разрешимости.

В данной статье всюду далее будем рассматривать класс $\mathcal{L}$ -КЛР-функций от n переменных исключительно при $\mathcal{L} = \{1, \dots, m-1\}$.

Утверждение 12. Для любых $m, n \in \mathbb{N}$ имеет место включение

$$\mathbf{CP}_{2^m}(n) \subseteq \mathbf{CLS}_{2^m}^{\mathcal{L}}(n). \quad (13)$$

Ясно, что класс всех ВКП-функций от n переменных над $\mathbb{Z}_{2^m}$ вкладывается в класс $\mathcal{L}$ -КЛР-функций в силу упомянутого ранее утверждения 3. Интересен тот факт, что имеет место включение, аналогичное теореме 1, а именно, класс $\mathcal{L}$ -КЛР-функций сохраняет отношение сравнимости по любому делителю 2^m .

Утверждение 13. Для любых $m, n \in \mathbb{N}$ имеет место включение

$$\mathbf{CLS}_{2^m}^{\mathcal{L}}(n) \subseteq \mathbf{D}_{2^m}(n).$$

Доказательство. Пусть $f(x_1, \dots, x_n) \in \mathbf{CLS}_{2^m}^{\mathcal{L}}(n)$ и $j \in \{1, \dots, m-1\}$. Покажем, что из сравнения $\alpha \equiv \beta \pmod{2^j}$, где $\alpha = (a_1, \dots, a_n)$, $\beta = (b_1, \dots, b_n) \in \mathbb{Z}_{2^m}^n$, следует $f(\alpha) \equiv f(\beta) \pmod{2^j}$.

Поскольку $a_i \equiv b_i \pmod{2^j}$ для любого $i \in \{1, \dots, n\}$, то при всех $l \in \{0, \dots, j-1\}$ верно равенство

$$a_i^{(l)} = b_i^{(l)}, \quad i = 1, \dots, n.$$

Тогда

$$g_0(a_1^{(0)}, \dots, a_n^{(0)}) = g_0(b_1^{(0)}, \dots, b_n^{(0)}),$$

и при $j > 1$ и $l \in \{1, \dots, j-1\}$

$$\begin{aligned} g_{li}(a_1^{(0)}, \dots, a_n^{(0)}, \dots, a_1^{(l-1)}, \dots, a_n^{(l-1)}) &= \\ &= g_{li}(b_1^{(0)}, \dots, b_n^{(0)}, \dots, b_1^{(l-1)}, \dots, b_n^{(l-1)}), \\ g_l(a_1^{(0)}, \dots, a_n^{(0)}, \dots, a_1^{(l-1)}, \dots, a_n^{(l-1)}) &= \\ &= g_l(b_1^{(0)}, \dots, b_n^{(0)}, \dots, b_1^{(l-1)}, \dots, b_n^{(l-1)}). \end{aligned}$$

Следовательно,

$$\gamma_l f(\alpha) = \gamma_l f(\beta), \quad l = 0, \dots, j-1.$$

А это, как легко видеть, равносильно сравнению $f(\alpha) \equiv f(\beta) \pmod{2^j}$. ■

Выше рассматривалось соотношение классов полиномиальных и ВКП-функций. Представляет также интерес вопрос о строгости включения $\mathbf{CP}_{2^m}(n)$ в класс $\mathbf{CLS}_{2^m}^{\mathcal{L}}(n)$. Ответ на него при $m \geq 3$ в определенной степени очевиден. Достаточно вспомнить, что, согласно утверждению 3, у ВКП-функций все g_{ji} несущественно зависят от $x_1^{(k)}, \dots, x_n^{(k)}$, где $k = \{1, \dots, j-1\}$. В то же время, при $m \geq 3$ легко привести пример координатных функций $\gamma_j f$, которые удовлетворяют условиям определения 7, но у которых g_{ji} существенно зависят хотя бы от одной из переменных $x_1^{(k)}, \dots, x_n^{(k)}$, где $k \in \{1, \dots, j-1\}$.

Также интересен вопрос о мощности класса $\mathcal{L}$ -КЛР-функций. В отличие от ВКП-функций можно найти ее точное значение.

Лемма 6. Число различных булевых функций $f(x_1, \dots, x_k, y_1, \dots, y_l)$ от $k+l$ переменных вида

$$\begin{aligned} f(x_1, \dots, x_k, y_1, \dots, y_l) &= \\ &= a_0(x_1, \dots, x_k) \oplus a_1(x_1, \dots, x_k)y_1 \oplus \dots \oplus a_l(x_1, \dots, x_k)y_l, \end{aligned}$$

где $a_i(x_1, \dots, x_k)$ ($i = 1, \dots, k$) — произвольные булевы функции, равно $2^{2^{k(l+1)}}$.

Доказательство. Очевидно, что разным наборам функций $(a_0(x_1, \dots, x_k), \dots, a_l(x_1, \dots, x_k))$ соответствуют различные функции $f(x_1, \dots, x_k, y_1, \dots, y_l)$. Следовательно, между ними существует взаимно-однозначное соответствие. Число же указанных наборов равно в точности $(2^{2^k})^{l+1} = 2^{2^{k(l+1)}}$. ■

Теорема 5. Для любых $m, n \in \mathbb{N}$ имеет место равенство

$$|\mathbf{CLS}_{2^m}^{\mathcal{L}}(n)| = 2^{2^n + (n+1) \frac{2^n(2^{n(m-1)} - 1)}{2^n - 1}}. \quad (14)$$

Доказательство. Число всех $\mathcal{L}$ -КЛР-функций равно произведению чисел j -х координатных отображений ($j = 0, \dots, m-1$). При $j = 0$ число нулевых координатных отображений есть число булевых функций от n переменных. При каждом $j = \{1, \dots, m-1\}$ количество различных j -х координатных отображений равно количеству булевых функций вида

$$\begin{aligned} \oplus \sum_{j=1}^n g_{ji} \left(x_1^{(0)}, \dots, x_n^{(0)}, \dots, x_1^{(j-1)}, \dots, x_n^{(j-1)} \right) \cdot x_i^{(j)} \oplus \\ \oplus g_j \left(x_1^{(0)}, \dots, x_n^{(0)}, \dots, x_1^{(j-1)}, \dots, x_n^{(j-1)} \right) \end{aligned}$$

и согласно доказанной лемме равно $2^{2^{jn}(n+1)}$.

Таким образом,

$$\begin{aligned} |\mathbf{CLS}_{2^m}^{\mathcal{L}}(n)| &= 2^{2^n} \prod_{j=1}^{m-1} 2^{2^{jn}(n+1)} = 2^{2^n} 2^{(n+1) \sum_{j=1}^{m-1} 2^{jn}} = 2^{2^n} 2^{(n+1) \frac{2^n(2^{n(m-1)} - 1)}{2^n - 1}} = \\ &= 2^{2^n + (n+1) \frac{2^n(2^{n(m-1)} - 1)}{2^n - 1}}. \blacksquare \end{aligned}$$

Из доказанной теоремы можно получить следующие следствия о соотношении классов $\mathcal{L}$ -КЛР и ВКП-функций.

Следствие. Для любого $n \in \mathbb{N}$ классы полиномиальных, ВКП-функций и $\mathcal{L}$ -КЛР-функций над $\mathbb{Z}_4$ от n переменных совпадают, т. е. $\mathbf{P}_4(n) = \mathbf{CP}_4(n) = \mathbf{CLS}_4^{\mathcal{L}}(n)$.

Доказательство. Данный факт следует из цепочки включений (в частности, из (13))

$$\mathbf{P}_4(n) \subseteq \mathbf{CP}_4(n) \subseteq \mathbf{CLS}_4^{\mathcal{L}}(n)$$

и равенства мощностей:

$$|\mathbf{P}_4(n)| = |\mathbf{CP}_4(n)| = |\mathbf{CLS}_4^{\mathcal{L}}(n)| = 2^{2^n(n+2)},$$

поскольку из (14) при $m = 2$ получим

$$|\mathbf{CLS}_4^{\mathcal{L}}(n)| = 2^{2^n + (n+1) \frac{2^n(2^n - 1)}{2^n - 1}} = 2^{2^n + (n+1)2^n} = 2^{2^n(n+2)}. \blacksquare$$

В соответствии с утверждением 13 любая $\mathcal{L}$ -КЛР-функция $f(x_1, \dots, x_n)$ сохраняет отношение сравнимости по делителям 2^m , поэтому данное условие является необходимым для принадлежности произвольной функции классу $\mathbf{CLS}_{2^m}^{\mathcal{L}}(n)$. В общем случае можно показать, что данное свойство не является достаточным. Однако для функций одной переменной оно является таковым.

Теорема 6. *Функция $f(x): \mathbb{Z}_{2^m} \rightarrow \mathbb{Z}_{2^m}$ является $\mathcal{L}$ -КЛР-функцией тогда и только тогда, когда она сохраняет отношение сравнимости по любому нетривиальному делителю 2^m .*

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

$$\begin{aligned} \gamma_j f(x) &= \gamma_j(f(x) \bmod 2^{j+1}) = \gamma_j(f(x \bmod 2^{j+1}) \bmod 2^{j+1}) = \\ &= \gamma_j(f(x^{(0)}, \dots, x^{(j)}) \bmod 2^{j+1}) = h_j(x^{(0)}, \dots, x^{(j)}), \end{aligned}$$

где $h_j(x^{(0)}, \dots, x^{(j)}): \mathcal{B}^j \rightarrow \mathcal{B}$ — некоторая булева функция от j переменных.

Таким образом при $j = 0$ функция $\gamma_0 f(x) = h_0(x^{(0)})$ является булевой от $x^{(0)}$. И в то же время при $j > 1$ функцию $h_j(x^{(0)}, \dots, x^{(j)})$ можно представить в виде

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

а это означает, что все $\gamma_j f(x) = h_j(x^{(0)}, \dots, x^{(j)})$ имеют вид, указанный в определении 7, и $f(x) \in \mathbf{CLS}_{2^m}^{\mathcal{L}}(1)$. ■

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

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

Доказательство. Равенства вытекают из следствия к теореме 5:

$$\mathbf{P}_4(1) = \mathbf{CP}_4(1) = \mathbf{CLS}_4^{\mathcal{L}}(1),$$

и из теоремы 6: $\mathbf{CLS}_4^{\mathcal{L}}(1) = \mathbf{D}_4(1)$. ■

Обозначим через $[\mathbf{CLS}_{2^m}^{\mathcal{L}}(n)]$ замыкание класса $\mathcal{L}$ -КЛР-функций, т. е. класс, получающийся путем всех возможных суперпозиций функций из $\mathbf{CLS}_{2^m}^{\mathcal{L}}(n)$. Пусть при этом, как и ранее, $\mathbf{x} = (x_1, \dots, x_n)$ и $\mathbf{x}^{(j)} = (x_1^{(j)}, \dots, x_n^{(j)})$ ($j \in \{0, \dots, m-1\}$).

Утверждение 14. При любых $m, n \in \mathbb{N}$ класс $\mathcal{L}$ -КЛР-функций $\mathbf{CLS}_{2^m}^{\mathcal{L}}(n)$ является замкнутым, т. е.

$$[\mathbf{CLS}_{2^m}^{\mathcal{L}}(n)] = \mathbf{CLS}_{2^m}^{\mathcal{L}}(n).$$

Доказательство. Покажем, что если функции $f, h_1, \dots, h_n \in \mathbf{CLS}_{2^m}^{\mathcal{L}}(n)$, то $u = f(h_1, \dots, h_n) \in \mathbf{CLS}_{2^m}^{\mathcal{L}}(n)$. Обозначим через g_j^f, g_{ji}^f и $g_j^{h_l}, g_{ji}^{h_l}$ ($l = 1, \dots, n$) булевы функции из определения 7 для f и h_l соответственно. Тогда

$$\begin{aligned} \gamma_0 u(\mathbf{x}) &= \gamma_0 f(h_1(\mathbf{x}), \dots, h_n(\mathbf{x})) = \\ &= g_0^f(\gamma_0 h_1(\mathbf{x}), \dots, \gamma_0 h_n(\mathbf{x})) = g_0^f(g_0^{h_1}(\mathbf{x}^{(0)}), \dots, g_0^{h_n}(\mathbf{x}^{(0)})) = g_0^u(\mathbf{x}^{(0)}). \end{aligned}$$

Если $j \in \{1, \dots, m-1\}$, то

$$\begin{aligned} \gamma_j u(\mathbf{x}) &= \gamma_j f(h_1(\mathbf{x}), \dots, h_n(\mathbf{x})) = \\ &= \oplus \sum_{i=1}^n g_{ji}^f(\gamma_0 h_1(\mathbf{x}), \dots, \gamma_0 h_n(\mathbf{x}), \dots, \gamma_{j-1} h_1(\mathbf{x}), \dots, \gamma_{j-1} h_n(\mathbf{x})) \cdot \gamma_j h_i(\mathbf{x}) \oplus \\ &\quad \oplus g_j^f(\gamma_0 h_1(\mathbf{x}), \dots, \gamma_0 h_n(\mathbf{x}), \dots, \gamma_{j-1} h_1(\mathbf{x}), \dots, \gamma_{j-1} h_n(\mathbf{x})). \end{aligned}$$

Каждая из координатных функций $\gamma_k h_l(\mathbf{x})$ ($l = 1, \dots, n, k = 0, \dots, j$) зависит от координат переменных $x_1^{(0)}, \dots, x_n^{(0)}, \dots, x_1^{(k)}, \dots, x_n^{(k)}$, поэтому выражения

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

и

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

зависят только от $x_1^{(0)}, \dots, x_n^{(0)}, \dots, x_1^{(j-1)}, \dots, x_n^{(j-1)}$. Следовательно,

$$\begin{aligned} \gamma_j u(\mathbf{x}) &= \oplus \sum_{i=1}^n r_{ji}(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j-1)}) \cdot \gamma_j h_i(\mathbf{x}) \oplus r_j(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j-1)}) = \\ &= \oplus \sum_{i=1}^n r_{ji}(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j-1)}) \times \\ &\quad \times \left(\sum_{k=1}^n g_{ji}^{h_i}(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j-1)}) \cdot x_k^{(j)} \oplus g_j^{h_i}(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j-1)}) \right) \oplus \\ &\quad \oplus r_j(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j-1)}) = \oplus \sum_{i=1}^n g_{ji}^u(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j-1)}) \cdot x_i^{(j)} \oplus g_j^u(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j-1)}). \end{aligned}$$

Таким образом, каждая координатная функция $\gamma_i u$ удовлетворяет условиям определения 7, а значит, функция u обладает свойством координатно-линейной разрешимости. ■

§ 3. Решение систем $\mathcal{L}$ -КЛР и ВКП-уравнений

В данном параграфе речь пойдет о решении систем $\mathcal{L}$ -КЛР-уравнений над $\mathbb{Z}_{2^m}$ ($m > 1$), т. е. систем

$$\begin{cases} \dots \\ f(x_1, \dots, x_n) = y, \\ \dots \end{cases}$$

у которых функции $f(x_1, \dots, x_n)$, стоящие в левой части каждого уравнения, являются $\mathcal{L}$ -КЛР-функциями. В частности 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 $f \in \mathbf{CLS}_{2^m}^{\mathcal{L}}(n)$ и $y \in \mathbb{Z}_{2^m}$, то уравнение $f(x_1, \dots, x_n) = y$ после приведения его левой и правой частей по модулю 2 примет вид

$$\begin{aligned} f(x_1, \dots, x_n) \equiv y \pmod{2} &\Leftrightarrow \gamma_0 f(x_1, \dots, x_n) = y^{(0)} \Leftrightarrow \gamma_0 f(\mathbf{x}^{(0)}) = y^{(0)} \Leftrightarrow \\ &\Leftrightarrow g(x_1^{(0)}, \dots, x_n^{(0)}) = y^{(0)}. \end{aligned}$$

Следовательно, после приведения по модулю 2 оно становится равносильным некоторому булеву уравнению от переменных $x_1^{(0)}, \dots, x_n^{(0)}$. При этом, чтобы найти функцию g_0 , достаточно привести по модулю 2 значения функции f на множестве $\mathcal{B}^n$.

Если $f \in \mathbf{CLS}_{2^m}^{\mathcal{L}}(n)$, $y \in \mathbb{Z}_{2^m}$ и $j \in \{0, \dots, m-2\}$, то уравнение $f(x_1, \dots, x_n) = y$ после приведения по модулю 2^{j+1} примет вид

$$\begin{aligned} f(x_1, \dots, x_n) &\equiv y \pmod{2^{j+1}} \Leftrightarrow \\ &\Leftrightarrow \gamma_0 f(\mathbf{x}) + \dots + 2^j \gamma_j f(\mathbf{x}) = y^{(0)} + \dots + 2^j y^{(j)} \Leftrightarrow \\ &\Leftrightarrow \begin{cases} \gamma_0 f(\mathbf{x}) = y^{(0)}, \\ \gamma_1 f(\mathbf{x}) = y^{(1)}, \\ \vdots \\ \gamma_j f(\mathbf{x}) = y^{(j)}. \end{cases} \end{aligned}$$

Поскольку при любом $l \in \{0, \dots, j\}$ координатная функция $\gamma_l f(\mathbf{x})$ зависит только от $\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(l)}$, то полученное можно записать следующим образом:

$$\begin{cases} \gamma_0 f(\mathbf{x}^{(0)}) = y^{(0)}, \\ \gamma_1 f(\mathbf{x}^{(0)}, \mathbf{x}^{(1)}) = y^{(1)}, \\ \vdots \\ \gamma_j f(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j)}) = y^{(j)}. \end{cases} \quad (15)$$

Пусть координаты $\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j-1)}$ удовлетворяют первым j уравнениям (15), тогда для решения (15) необходимо и достаточно решить уравнение

$$\gamma_j f(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j)}) = y^{(j)} \quad (16)$$

относительно $\mathbf{x}^{(j)}$. При этом (16) является линейным по $\mathbf{x}^{(j)}$ при любых фиксированных координатах $\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j-1)}$, поскольку согласно свойству координатно-линейной разрешимости (16) есть в точности уравнение вида

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

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

Пусть теперь задана система $\mathcal{L}$ -КЛР-уравнений от n переменных $x_1, \dots, x_n$

$$\begin{cases} \dots \\ f(x_1, \dots, x_n) = y, \\ \dots \end{cases} \quad (17)$$

над $\mathbb{Z}_{2^m}$ ($m > 1$); опишем алгоритм нахождения ее решений.

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

$$f(x_1, \dots, x_n) = y$$

и приведем его по модулю 2. Согласно проведенным ранее рассуждениям, получим булево уравнение

$$\gamma_0 f(\mathbf{x}^{(0)}) = y^{(0)} \Leftrightarrow g_0(x_1^{(0)}, \dots, x_n^{(0)}) = y^{(0)}$$

относительно младших координат $x_1^{(0)}, \dots, x_n^{(0)}$. Приводя таким же образом каждое уравнение в (17), придем к некоторой системе булевых уравнений

относительно $x_1^{(0)}, \dots, x_n^{(0)}$. Решаем данную систему и находим возможные значения младших координат.

2. Пусть при $j \in \{1, \dots, m-1\}$ найдены значения координат переменных $\mathbf{x}^{(0)} = \mathbf{c}^{(0)}, \dots, \mathbf{x}^{(j-1)} = \mathbf{c}^{(j-1)}$, которые для каждого уравнения $f(x_1, \dots, x_n) = y$ системы (17) удовлетворяют равенствам

$$\begin{cases} \gamma_0 f(\mathbf{c}^{(0)}) = y^{(0)}, \\ \gamma_1 f(\mathbf{c}^{(0)}, \mathbf{c}^{(1)}) = y^{(1)}, \\ \vdots \\ \gamma_{j-1} f(\mathbf{c}^{(0)}, \dots, \mathbf{c}^{(j-1)}) = y^{(j-1)}. \end{cases} \quad (18)$$

Если $j = m$, то перейти к п. 4. Иначе при любом таком наборе координат неизвестных $\mathbf{c}^{(0)}, \dots, \mathbf{c}^{(j-1)}$ выполним следующие действия. Приводя данное уравнение по модулю 2^{j+1} , получим соотношение

$$\begin{aligned} \gamma_j f(\mathbf{c}^{(0)}, \dots, \mathbf{c}^{(j-1)}, \mathbf{x}^{(j)}) &= y^{(j)} \Leftrightarrow \\ \Leftrightarrow \sum_{i=1}^n g_{ji}(\mathbf{c}^{(0)}, \dots, \mathbf{c}^{(j-1)}) \cdot x_i^{(j)} \oplus g_j(\mathbf{c}^{(0)}, \dots, \mathbf{c}^{(j-1)}) &= y^{(j)}, \end{aligned} \quad (19)$$

которое при любых фиксированных наборах значений $\mathbf{c}^{(0)}, \dots, \mathbf{c}^{(j-1)}$ является линейным. Это означает, что существуют такие a_{ji} , $a_j \in \mathcal{B}$ ($i = 1, \dots, n$), что (19) имеет вид

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

Чтобы найти эти коэффициенты (при фиксированных $\mathbf{c}^{(0)}, \dots, \mathbf{c}^{(j-1)}$), очевидно, достаточно вычислить значения $\gamma_j f(\mathbf{c}^{(0)}, \dots, \mathbf{c}^{(j-1)}, \mathbf{x}^{(j)})$ как функции от $\mathbf{x}^{(j)}$ на наборах $\{\theta = (0, \dots, 0), \theta_i = (0, \dots, 1, \dots, 0), i = 1, \dots, n\}$. Таким образом, каждое уравнение исходной системы приводит к некоторому линейному уравнению над полем $\mathcal{B}$ относительно неизвестных $x_1^{(j)}, \dots, x_n^{(j)}$. 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 (18), необходимо найти все возможные значения координат $\mathbf{x}^{(j)}$. Если таких $\mathbf{x}^{(j)}$ нет, то исходная система (17) несовместна и алгоритм заканчивает работу. В противном случае увеличить j на 1 и перейти к п. 2.

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

$$\mathbf{c} = \sum_{j=0}^{m-1} 2^j \cdot \mathbf{c}^{(j)},$$

и на этом алгоритм завершает свою работу.

Утверждение 15. *Приведенный алгоритм корректен, то есть находит все решения системы (17) либо определяет ее несовместность.*

Доказательство. Корректность алгоритма следует из того, что $\mathbf{c} = (c_1, \dots, c_n)$ является решением (17) в том и только в том случае, когда для любого уравнения этой системы $f(x_1, \dots, x_n) = y$ выполняются равенства

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

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

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

для любого уравнения $f(x_1, \dots, x_n) = y$ 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 $x_1^{(j)}, \dots, x_n^{(j)}$ ($j \in \{1, \dots, m - 1\}$), как видно, требуется решить систему линейных уравнений над полем $\mathcal{B}$. В предположении, что в системе порядка $O(n)$ уравнений, ее решение методом Гаусса имеет сложность $O(n^3)$. Кроме того, чтобы получить саму эту систему, необходимо найти линейное представление $a_{j1}x_1^{(j)} \oplus \dots \oplus a_{jn}x_n^{(j)} \oplus a_j = y^{(j)}$ для каждого ее уравнения. Очевидно, что для одного уравнения это можно сделать за $n + 1$ операций (считая,

что вычисление значения функции 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 $j \neq 0$).

Список литературы

1. Глухов М. М., Шишков А. Б. Математическая логика. Дискретные функции. Теория алгоритмов. — М.: Лань, 2012.
2. 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.
3. Михайлов Д. А. Решение некоторых классов систем полиномиальных уравнений над конечными полями и кольцами // Труды по дискретной математике. — 2008. — Т. 11. — С. 125–146.
4. Нечаев А. А. Полиномиальные преобразования конечных коммутативных локальных колец главных идеалов // Матем. заметки. — 1980. — Т. 27. Вып. 6 — С. 885–899.
5. Anashin V., Khrennikov A. Applied Algebraic Dynamics // de Gruyter Expositions in Mathematics. — Walter de Gruyter, Berlin–New York, 2009. — V. 49.
6. Анашин В. С. Равномерно распределенные последовательности целых p -адических чисел // Дискретная математика. — 2002. — Т. 14. Вып. 4. — С. 3–64.