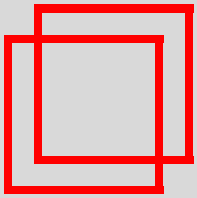
Math-Net.Ru
Общероссийский математический портал

А. Б. Ремизов, О надструктуре замкнутого класса полиномов по модулю k, *Дискрет. матем.*, 1989, том 1, выпуск 1, 3–15

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: 3.22.242.169
10 января 2025 г., 17:02:01

Дискретная математика

том 1 выпуск 1 * 1989

УДК 519.716

О НАДСТРУКТУРЕ ЗАМКНУТОГО КЛАССА ПОЛИНОМОВ ПО МОДУЛЮ k

А. Б. Ремизов

Пусть $\mathcal{P}_k$ — класс k-значных функций, представимых полиномами над кольцом вычетов $\mathbf{Z}_k$, а $\mathfrak{M}_k$ — замкнутый класс функций, сохраняющих все конгруэнции кольца $\mathbf{Z}_k$. В работе показано, что решетка замкнутых классов, лежащих между $\mathcal{P}_k$ и $\mathfrak{M}_k$, при $k = p_1^2 \dots p_s^2 p_{s+1} \dots p_l$, $p_i \neq p_j$, свободном от кубов простых чисел, конечна и изоморфна s-мерному кубу, а при $k = p^3 q$, $p > 1$, $q \geqslant 1$ эта решетка бесконечна.

Настоящая работа относится к направлению в теории k-значных функций, которое занимается изучением свойств решетки замкнутых классов в P_k [13]. Значительная сложность этой решетки при $k \geqslant 3$, связанная, в частности, с континуальностью множества ее элементов, наличием в ней замкнутых классов без конечного базиса [14], вынудила исследователей интересоваться отдельными ее фрагментами. В основном изучались первый и второй уровни решетки (предполные и предпредполные классы) [16, 17], а также надструктуры наиболее известных классов — линейных и самодвойственных функций [4, 18], класса $\mathcal{P}_k$ полиномов над кольцом вычетов $\mathbf{Z}_k$.

В настоящей работе продолжается исследование надструктуры класса полиномов $\mathcal{P}_k$, начатое С. В. Яблонским [13] и получившее свое развитие в работах А. А. Нечаева [8], А. Н. Черепова [11, 12] и Д. Г. Мещанинова [5—7]. Напомним основные результаты этих работ, относящиеся к описанию надструктуры класса $\mathcal{P}_k$.

В [13] было показано, что при простом k любая функция k-значной логики представима полиномом по модулю k, т. е. $P_k = \mathcal{P}_k$, тогда как при составном k класс полиномов даже не предполон.

В работе [8] получены условия полноты системы k-значных функций, содержащей операции кольца $\mathbf{Z}_k$, т. е., другими словами, описаны все предполные классы, содержащие $\mathcal{P}_k$. Ими оказались классы всех функций, сохраняющих отношение сравнения по модулю d для каждого собственного делителя d числа k.

Очевидно, что класс полиномов $\mathcal{P}_k$ содержится в пересечении $\mathfrak{M}_k$ всех предполных классов, включающих в себя $\mathcal{P}_k$. Класс $\mathfrak{M}_k$ состоит из k-значных функций, сохраняющих любое отношение сравнения по модулю d, где d — собственный делитель k, или, другими словами, из функций, сохраняющих конгруэнции кольца вычетов $\mathbf{Z}_k$. В работе [1] показано, что при составном k, свободном от квадратов простых чисел, имеет место равенство $\mathcal{P}_k = \mathfrak{M}_k$. При тех же ограничениях на k в [11] получено описание надструктуры класса $\mathcal{P}_k$.

© Издательство «Наука». Главная редакция физико-математической литературы, «Дискретная математика», 1989

В работе [6] рассматривался случай, когда $k=p_1^2p_2\ldots p_s$, где $p_1, p_2, \ldots, p_s$—различные простые числа. Автор показал, что в этом случае класс полиномов предполон в $\mathfrak{M}_k$, а при $k=p_1^2p_2$ полностью описал надструктуру класса $\mathcal{P}_k$.

Таким образом, изучение надструктуры класса $\mathcal{P}_k$ велось, в основном, в двух направлениях: описание надструктуры класса $\mathfrak{M}_k$ и описание решетки $[\mathcal{P}_k; \mathfrak{M}_k]$ замкнутых классов, лежащих между $\mathcal{P}_k$ и $\mathfrak{M}_k$.

В настоящей работе получено полное описание решетки $[\mathcal{P}_k; \mathfrak{M}_k]$ при k, свободном от кубов простых чисел. В случае $k=p^3q$, $p>1$, $q\geqslant 1$, построена счетная цепочка замкнутых классов между $\mathcal{P}_k$ и $\mathfrak{M}_k$, указан замкнутый класс без конечного базиса, содержащий класс полиномов. Последний факт является косвенным подтверждением значительной сложности надструктуры класса полиномов $\mathcal{P}_k$ при произвольном k.

§ 1. Свойства замкнутого класса $\mathfrak{M}_k$

В этом параграфе мы изучим основные свойства класса $\mathfrak{M}_k$, состоящего из k-значных функций, сохраняющих все конгруэнции кольца $\mathbf{Z}_k$, укажем базис в этом классе и критерий принадлежности произвольной функции классу $\mathfrak{M}_k$. Вначале напомним основные определения и обозначения.

Пусть $\Omega_k=\{0, 1, \ldots, k-1\}$. Функция k-значной логики $f(x_1, \ldots, x_n)$—это отображение декартовой степени Ω_k^n множества Ω_k в множество Ω_k. Множество функций k-значной логики, как это принято, мы будем обозначать через P_k. Понятия суперпозиции k-значных функций и замыкания системы функций $\Phi\subseteq P_k$ вводятся обычным образом (см., например, [3, 13]). Замыкание системы $\Phi\subseteq P_k$ мы иногда будем обозначать через $[\Phi]_k$, подчеркивая тем самым принадлежность системы Φ множеству P_k.

Класс полиномов $\mathcal{P}_k$ над кольцом вычетов $\mathbf{Z}_k$, очевидно, является замыканием системы функций $\{\mathbf{1}, x+y, x\cdot y\}$, где $\mathbf{1}$—функция-константа, равная 1, а $x+y$, $x\cdot y$—соответственно операции сложения и умножения по модулю k. Из результатов работы [17] следует, что единственными предполными классами [13], содержащими $\mathcal{P}_k$, являются семейства $\mathfrak{U}_k^{(d)}$ функций, сохраняющих отношение сравнения по модулю d, где d делит k и $d\neq 1$, $d\neq k$. Пусть

$$\mathfrak{M}_k=\bigcap_{\substack{d\mid k\\ d\neq 1,\ k}}\mathfrak{U}_k^{(d)}.$$

Тогда $\mathfrak{M}_k$ состоит из всех функций $f(x_1, \ldots, x_n)\in P_k$ $(n\in\mathbf{N})$ таких, что из

$$a_1\equiv b_1 \pmod d,\quad \ldots,\quad a_n\equiv b_n \pmod d$$

следует $f(a_1, \ldots, a_n)\equiv f(b_1, \ldots, b_n) \pmod d$ для любого d—собственного делителя k. Отметим, что $\mathcal{P}_k\subseteq\mathfrak{M}_k$, а при k, свободном от квадратов простых чисел, имеет место равенство $\mathcal{P}_k=\mathfrak{M}_k$ [1].

Следуя [8], введем определения компоненты k-значной функции и координаты p^m-значной функции.

Определение 1. Пусть $f(x_1, \ldots, x_n)\in P_k$ и $k=rs$, где $r, s>1$. Тогда *r-компонентой* функции f назовем r-значную функцию $f^{(r)}$, действующую из Ω_k^n в Ω_r и определяемую равенством

$$f^{(r)}(x_1, \ldots, x_n)\equiv f(x_1, \ldots, x_n) \pmod r.$$

Если $k=p_1^{\alpha_1}\ldots p_s^{\alpha_s}$, где $p_1, \ldots, p_s$—различные простые числа, то на основании «китайской» теоремы об остатках [2] любая k-значная функция $f(x_1, \ldots, x_n)$ однозначно определяется своими $p_i^{\alpha_i}$-компонентами $f^{(p_1^{\alpha_1})}(x_1, \ldots, x_n), \ldots, f^{(p_s^{\alpha_s})}(x_1, \ldots, x_n)$. В дальнейшем при наличии фиксиро-

ванного порядка следования простых чисел в разложении $p_1^{\alpha_1} \dots p_s^{\alpha_s}$ числа k мы будем использовать следующую запись компонент функции f: $f^{(1)}, \dots, f^{(s)}$.

Определение 2. Пусть $f(x_1, \dots, x_n) \in P_k$ и $k = p^m$. Тогда p-значные функции $\delta_0(f)(x_1, \dots, x_n), \dots, \delta_{m-1}(f)(x_1, \dots, x_n)$, удовлетворяющие равенству

$$f(x_1, \dots, x_n) = \sum_{j=0}^{m-1} p^j \delta_j(f),$$

называются *координатными функциями* функции f. Отметим, что каждая координатная функция $\delta_i(f)$ является функцией p-значной логики от nm переменных $\delta_0(x_1), \dots, \delta_{m-1}(x_1), \dots, \delta_0(x_n), \dots, \delta_{m-1}(x_n)$, принимающих свои значения в Ω_p.

На языке компонент и координатных функций несложно описываются функции из класса $\mathfrak{M}_k$.

Теорема 1. *Пусть $k = p_1^{\alpha_1} \dots p_s^{\alpha_s}$, где $p_1, \dots, p_s$ — различные простые числа. Функция $f(x_1, \dots, x_n)$ принадлежит классу $\mathfrak{M}_k$ в том и только том случае, если любая ее компонента $f^{(i)}$ имеет вид*

$$f^{(i)}(x_1, \dots, x_n) = f^{(i)}(x_1^{(i)}, \dots, x_n^{(i)}) = \sum_{j=0}^{\alpha_i - 1} p_i^j \delta_j(f^{(i)}), \qquad (1)$$

где $\delta_j(f^{(i)}) = \delta_j(f^{(i)})(\delta_0(x_1^{(i)}), \dots, \delta_j(x_1^{(i)}), \dots, \delta_0(x_n^{(i)}), \dots, \delta_j(x_n^{(i)}))$, $j \in \{0, 1, \dots, \alpha_i - 1\}$, $i \in \{1, \dots, s\}$.

Доказательство. Пусть $f(x_1, \dots, x_n) \in \mathfrak{M}_k$. Тогда для любого $i \in \{1, \dots, s\}$ из равенств

$$x_1 \equiv y_1 \pmod{p_i^{\alpha_i}}, \quad \dots, \quad x_n \equiv y_n \pmod{p_i^{\alpha_i}}$$

следует $f(x_1, \dots, x_n) = f(y_1, \dots, y_n) \pmod{p_i^{\alpha_i}}$. Это означает, что $p_i^{\alpha_i}$-компонента функции f существенно зависит лишь от $p_i^{\alpha_i}$-компонент переменных $x_1, \dots, x_n$. Запишем функцию $f(x_1, \dots, x_n)$ в виде

$$f(x_1, \dots, x_n) = \sum_{j=0}^{\alpha_i - 1} p_i^j \delta_j(f^{(i)})(x_1^{(i)}, \dots, x_n^{(i)}) + p_i^{\alpha_i} g(x_1, \dots, x_n).$$

Так как по условию функция f сохраняет отношения сравнения по модулям $p_i, p_i^2, \dots, p_i^{\alpha_i - 1}$, то каждая координатная функция $\delta_j(f^{(i)})$ существенно зависит лишь от координат переменных $x_1^{(i)}, \dots, x_n^{(i)}$ с номерами l, не превосходящими j:

$$\delta_j(f^{(i)}) = \delta_j(f^{(i)})(\delta_0(x_1^{(i)}), \dots, \delta_j(x_1^{(i)}), \dots, \delta_0(x_n^{(i)}), \dots, \delta_j(x_n^{(i)})).$$

Обратно, если компоненты функции $f(x_1, \dots, x_n)$ имеют вид (1), то функция f сохраняет отношения сравнения по любому примарному модулю $p_i^{\beta_i}$, $\beta_i \in \{1, \dots, \alpha_i\}$, $i \in \{1, \dots, s\}$. Но тогда на основании простейших свойств сравнений [2] функция f сохраняет отношение сравнения и по любому составному модулю $d = p_1^{\beta_1} \dots p_s^{\beta_s}$, где $0 \leqslant \beta_i \leqslant \alpha_i$, $i \in \{1, \dots, s\}$, т. е. принадлежит $\mathfrak{M}_k$.

Следствие. *При $k = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ функция $f(x_1, \dots, x_n)$ принадлежит классу $\mathfrak{M}_k$ в том и только том случае, если любая ее $p_i^{\alpha_i}$-компонента $f^{(i)}$ как $p_i^{\alpha_i}$-значная функция от $\alpha_i n$ переменных принадлежит классу $\mathfrak{M}_{p_i^{\alpha_i}}$.*

Таким образом, изучение класса $\mathfrak{M}_k$ при составном k может быть сведено к изучению классов $\mathfrak{M}_k$ при k, являющихся степенями простого числа.

Аналоги следствия из теоремы 1 справедливы и для некоторых других замкнутых классов. Например, отметим такой факт: функция f является полиномом по модулю k, где $k=p_1^{\alpha_1}\dots p_s^{\alpha_s}$, т. е. $f\in\mathcal{P}_k$ тогда и только тогда, когда $f^{(i)}\in\mathcal{P}_{p_i^{\alpha_i}}$, $i\in\{1,\dots,s\}$ (см., например, [1]).

Этот результат на самом деле является следствием более общего факта, связанного с описанием гомоморфных образов замкнутых классов, содержащихся в $\mathfrak{M}_k$. Вначале напомним понятие гомоморфизма замкнутого класса $\mathfrak{A}\subseteq P_k$ на замкнутый класс $\mathfrak{A}'\subseteq P_l$ (см. [13]).

Определение 3. Отображение ψ: $\mathfrak{A}\to\mathfrak{A}'$ называется *гомоморфизмом замкнутого класса* $\mathfrak{A}$ *в замкнутый класс* $\mathfrak{A}'$, если для любых функций $f(x_1,\dots,x_n)$, $f_1(x_{11},\dots,x_{1m_1}),\dots,f_n(x_{n1},\dots,x_{nm_n})\in\mathfrak{A}$ имеет место

$$\psi(f(f_1,\dots,f_n))=\psi(f)(\psi(f_1),\dots,\psi(f_n)).$$

Отметим, что гомоморфизм замкнутых классов можно определять и как гомоморфизм соответствующих подалгебр итеративной алгебры Поста [3]. С помощью гомоморфного отображения $\mathfrak{A}$ на $\mathfrak{A}'$ нередко удается переносить некоторые свойства класса $\mathfrak{A}$ на класс $\mathfrak{A}'$. В частности, поскольку гомоморфный (точнее, эпиморфный) образ замкнутого класса $\mathfrak{A}$ в $\mathfrak{A}'$ есть замкнутый класс в P_l, а прообраз любого замкнутого подкласса из $\mathfrak{A}'$ есть замкнутый класс в P_k [3], то решетка замкнутых классов, содержащихся в $\mathfrak{A}'$, иногда несет в себе значительную информацию о решетке замкнутых классов, содержащихся в $\mathfrak{A}$.

Непосредственно из определения гомоморфизма замкнутых классов следует

Лемма 1. *Если* ψ: $\mathfrak{A}\to\mathfrak{A}'$ *— эпиморфизм замкнутого класса* $\mathfrak{A}\subseteq P_k$ *на замкнутый класс* $\mathfrak{A}'\subseteq P_l$, *то для любой системы функций* $\Phi\subseteq\mathfrak{A}$

$$\psi([\Phi]_k)=[\psi(\Phi)]_l. \tag{2}$$

Нам потребуются следующие примеры гомоморфизмов замкнутых классов, на которые указал С. В. Яблонский [13].

Пусть $k=p_1^{\alpha_1}\dots p_s^{\alpha_s}$ и $\hat{\psi}_{\beta_i}$: $\mathbf{Z}_k\to\mathbf{Z}_{p_i^{\beta_i}}$ — гомоморфизм колец $\mathbf{Z}_k$ и $\mathbf{Z}_{p_i^{\beta_i}}$, задаваемый равенством

$$\hat{\psi}_{\beta_i}(x)\equiv x\,(\mathrm{mod}\,p_i^{\beta_i}),$$

где $\beta_i\in\{1,\dots,\alpha_i\}$, $i\in\{1,\dots,s\}$. Тогда гомоморфизмы $\hat{\psi}_{\beta_i}$ могут быть продолжены до гомоморфизмов ψ_{β_i} замкнутых классов $\mathfrak{M}_k$ и $\mathfrak{M}_{p_i^{\beta_i}}$. Для этого надо образом функции $f(x_1,\dots,x_n)\in\mathfrak{M}_k$ положить функцию $\psi_{\beta_i}(f)$, принимающую на наборе $(y_1,\dots,y_n)\in\Omega^n_{p_i^{\beta_i}}$ значение

$$\psi_{\beta_i}(f)(y_1,\dots,y_n)=\hat{\psi}_{\beta_i}(f(\hat{\psi}_{\beta_i}^{-1}(y_1),\dots,\hat{\psi}_{\beta_i}^{-1}(y_n))).$$

Здесь под $\hat{\psi}_{\beta_i}^{-1}(y)$ мы понимаем любой прообраз элемента $y\in\Omega_{p_i^{\beta_i}}$.

Действительно, непосредственно из определения ψ_{β_i} следует, что для произвольной функции $f(x_1,\dots,x_n)\in\mathfrak{M}_k$ справедливо равенство

$$\psi_{\beta_i}(f)=\sum_{j=0}^{\beta_i-1}p_i^j\delta_j(f^{(i)})(x_1^{(i)},\dots,x_n^{(i)}).$$

По следствию из теоремы 1 это означает, что образом множества $\mathfrak{M}_k$ при действии ψ_{β_i} является класс $\mathfrak{M}_{p_i^{\beta_i}}$. Свойство отображения ψ_{β_i} «выдерживать» операцию суперпозиции проверяется непосредственно, как и в [13].

Построенные гомоморфизмы $\psi_{\alpha_i}\colon \mathfrak{M}_k \to \mathfrak{M}_{p_i^{\alpha_i}}$, $i \in \{1, \ldots, s\}$, позволяют изучать решетку замкнутых классов из $\mathfrak{M}_{p_i^{\alpha_i}}$ по решетке замкнутых классов из $\mathfrak{M}_k$. Следующая теорема показывает, что верно и обратное, т. е. по структуре классов $\mathfrak{M}_{p_1^{\alpha_1}}, \ldots, \mathfrak{M}_{p_s^{\alpha_s}}$ можно полностью описать и структуру класса $\mathfrak{M}_k$.

Теорема 2. *Пусть* $k = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$, *где* $p_1, \ldots, p_s$ — *различные простые числа. Тогда справедливы следующие утверждения.*

1. *Любому набору замкнутых классов* $\mathfrak{A}_i \subseteq \mathfrak{M}_{p_i^{\alpha_i}}$, $i \in \{1, \ldots, s\}$, *соответствует замкнутый класс* $\mathfrak{M}_k^{\mathfrak{A}_1, \ldots, \mathfrak{A}_s}$, *где*

$$\mathfrak{M}_k^{\mathfrak{A}_1, \ldots, \mathfrak{A}_s} = \{f \in \mathfrak{M}_k \mid f^{(i)} \in \mathfrak{A}_i, \quad i \in \{1, \ldots, s\}\}. \tag{3}$$

2. *Для любого замкнутого класса* $\mathfrak{N} \subseteq \mathfrak{M}_k$, *содержащего класс линейных функций* $\mathscr{L}_k = [x+y]_k$, *существует единственный набор замкнутых классов* $\mathfrak{A}_i$, $\mathscr{L}_{p_i^{\alpha_i}} \subseteq \mathfrak{A}_i \subseteq \mathfrak{M}_{p_i^{\alpha_i}}$, $i \in \{1, \ldots, s\}$, *такой, что*

$$\mathfrak{N} = \mathfrak{M}_k^{\mathfrak{A}_1, \ldots, \mathfrak{A}_s}.$$

Доказательство. 1. Замкнутость класса $\mathfrak{M}_k^{\mathfrak{A}_1, \ldots, \mathfrak{A}_s}$ очевидна.

2. Пусть $\mathfrak{N}$ — произвольный замкнутый класс в $\mathfrak{M}_k$, содержащий $\mathscr{L}_k$. Тогда для каждого $i \in \{1, \ldots, s\}$ класс $\psi_{\alpha_i}(\mathfrak{N}) = \mathfrak{A}_i$ является замкнутым и содержащимся в $\mathfrak{M}_{p_i^{\alpha_i}}$. Так как $\mathscr{L}_k \subseteq \mathfrak{N}$, то по лемме 1 имеем $\psi_{\alpha_i}(\mathfrak{N}) \supseteq \supseteq [\psi_{\alpha_i}(x+y)]_{p_i^{\alpha_i}}$. Следовательно, $\mathfrak{A}_i \supseteq \mathscr{L}_{p_i^{\alpha_i}}$, $i \in \{1, \ldots, s\}$. Несложно проверить, что $\mathfrak{N} \subseteq \mathfrak{M}_k^{\mathfrak{A}_1, \ldots, \mathfrak{A}_s}$. Покажем, что на самом деле имеет место равенство $\mathfrak{N} = \mathfrak{M}_k^{\mathfrak{A}_1, \ldots, \mathfrak{A}_s}$.

Возьмем произвольную функцию $f(x_1, \ldots, x_n) \in \mathfrak{M}_k^{\mathfrak{A}_1, \ldots, \mathfrak{A}_s}$. Тогда $\psi_{\alpha_i}(f) = f^{(i)} \in \mathfrak{A}_i$, $i \in \{1, \ldots, s\}$. Но $\mathfrak{A}_i = \psi_{\alpha_i}(\mathfrak{N})$. Следовательно, существуют функции $h_i(x_1, \ldots, x_n) \in \mathfrak{N}$, $i \in \{1, \ldots, s\}$, такие, что

$$\psi_{\alpha_i}(f) = \psi_{\alpha_i}(h_i), \qquad i \in \{1, \ldots, s\}.$$

Так как класс $\mathfrak{N}$ содержит линейные функции, то в нем найдется линейная функция $t(x_1, \ldots, x_s)$ такая, что

$$\psi_{\alpha_i}(t(x_1, \ldots, x_s)) = x_i^{(i)}, \qquad i \in \{1, \ldots, s\}.$$

Нетрудно проверить, что этим равенствам удовлетворяет функция

$$t(x_1, \ldots, x_s) = a_1 p_2^{\alpha_2} \ldots p_s^{\alpha_s} x_1 + a_2 p_1^{\alpha_1} p_3^{\alpha_3} \ldots p_s^{\alpha_s} x_2 + \ldots + a_s p_1^{\alpha_1} \ldots p_{s-1}^{\alpha_{s-1}} x_s,$$

где $a_i p_1^{\alpha_1} \ldots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \ldots p_s^{\alpha_s} \equiv 1 \pmod{p_i^{\alpha_i}}$, $i \in \{1, \ldots, s\}$. Тогда $t(h_1(x_1, \ldots, x_n), \ldots, h_s(x_1, \ldots, x_n)) \in \mathfrak{N}$ и для любого $i \in \{1, \ldots, s\}$ выполнено равенство

$$\psi_{\alpha_i}(f(x_1, \ldots, x_n)) = \psi_{\alpha_i}(t(h_1(x_1, \ldots, x_n), \ldots, h_s(x_1, \ldots, x_n))).$$

Так как по своим компонентам функция восстанавливается однозначно, то

$$f(x_1, \ldots, x_n) = t(h_1(x_1, \ldots, x_n), \ldots, h_s(x_1, \ldots, x_n))$$

и $f \in \mathfrak{N}$. Следовательно, $\mathfrak{N} = \mathfrak{M}_k^{\mathfrak{A}_1, \ldots, \mathfrak{A}_s}$. Теорема доказана.

Главный вывод, который можно сделать из теоремы 2, таков: решетка замкнутых классов, лежащих между классом линейных функций $\mathscr{L}_k$ и

классом $\mathfrak{M}_k$, при $k=p_1^{\alpha_1}\dots p_s^{\alpha_s}$ однозначно определяется решетками замкнутых классов $\left[\mathscr{L}_{p_i^{\alpha_i}};\ \mathfrak{M}_{p_i^{\alpha_i}}\right]$, $i\in\{1,\ \dots,\ s\}$. В связи с этим более подробно остановимся на свойствах замкнутого класса $\mathfrak{M}_k$ при $k=p^m$.

Пусть $k=p^m$. Рассмотрим систему функций

$$\Phi_{p^m}=\{1,\ x+y,\ \delta_0(x)\,\delta_0(y),\ \dots,\ p^{m-1}\delta_{m-1}(x)\,\delta_{m-1}(y)\},\qquad(4)$$

где $p^i\delta_i(x)\,\delta_i(y)$—функция, у которой все координаты, кроме i-й, равны нулю, а i-я координата равна $\delta_i(x)\,\delta_i(y)\,(\mathrm{mod}\,p)$.

Теорема 3. *Система Φ_{p^m} является базисом замкнутого класса $\mathfrak{M}_{p^m}$.*

Доказательство. Воспользуемся индукцией по m. При $m=1$ система $\Phi_p=\{1,\ x+y,\ x\cdot y\}$ полна в P_p, а, следовательно, и в $\mathfrak{M}_p$.

Предположим, что утверждение теоремы доказано для функций p^{m-1}-значной логики, и докажем ее для p^m-значных функций. Пусть $f(x_1,\ \dots,\ x_n)\in\in\mathfrak{M}_{p^m}$. Запишем функцию f в виде

$$f(x_1,\ \dots,\ x_n)=f_1(x_1,\ \dots,\ x_n)+p^{m-1}g(x_1,\ \dots,\ x_n),$$

где f_1—p^{m-1}-компонента функции f. В силу теоремы 1 выполнено включение $f_1\in\mathfrak{M}_{p^{m-1}}$. По предположению индукции $f_1\in[\Phi_{p^{m-1}}]$.

Заметим, что все операции системы $\Phi_{p^{m-1}}$ принадлежат классу $[\Phi_{p^m}]$. Для функций $p^i\delta_i(x)\,\delta_i(y)$, $i\in\{0,\ \dots,\ m-2\}$, этот факт является очевидным. Операция сложения $x_{m-1}+y$ по модулю p^{m-1} выражается через сложение x_m+y по модулю p^m и функции системы Φ_{p^m} следующим образом:

$$x_{m-1}+y=x_m+y_m-p^{m-1}\delta_{m-1}(x_m+y),$$
$$p^{m-1}\delta_{m-1}(x)=p^{m-1}\underbrace{\delta_{m-1}(x)\dots\delta_{m-1}(x)}_{p\text{ раз}}.$$

Следовательно, $f_1\in[\Phi_{p^m}]$.

Осталось показать, что функция $p^{m-1}g(x_1,\ \dots,\ x_n)$ принадлежит классу $[\Phi_{p^m}]$. Воспользуемся тем фактом, что любая p-значная функция, в частности функция $g(\delta_0(x_1),\ \dots,\ \delta_{m-1}(x_1),\ \dots,\ \delta_0(x_n),\ \dots,\ \delta_{m-1}(x_n))$, представима полиномом по модулю p от переменных $\delta_0(x_1),\ \dots,\ \delta_{m-1}(x_1),\ \dots\ \dots,\ \delta_0(x_n),\ \dots,\ \delta_{m-1}(x_n)$:

$$g(x_1,\ \dots,\ x_n)=\sum_{\alpha_{1,0},\ \dots,\ \alpha_{n,m-1}=0}^{p-1}a_{\alpha_{1,0},\ \dots,\ \alpha_{n,m-1}}\delta_0^{\alpha_{1,0}}(x_1)\dots$$
$$\dots\delta_{m-1}^{\alpha_{1,m-1}}(x_1)\dots\delta_{m-1}^{\alpha_{n,m-1}}(x_n),$$

где $\sum$—сложение по модулю p. Несложно проверить, что

$$p^{m-1}g(x_1,\ \dots,\ x_n)=$$
$$=p^{m-1}\sum_{\alpha_{1,0},\ \dots,\ \alpha_{n,m-1}=0}^{p-1}a_{\alpha_{1,0},\ \dots,\ \alpha_{n,m-1}}\delta_0^{\alpha_{1,0}}(x_1)\dots\delta_{m-1}^{\alpha_{1,m-1}}(x_1)\dots\delta_{m-1}^{\alpha_{n,m-1}}(x_n),$$

где $\sum$—уже́ сложение по модулю p^m.

Для доказательства теоремы 3 достаточно показать, что каждое слагаемое

$$p^{m-1}a_{\alpha_{1,0},\ \dots,\ \alpha_{n,m-1}}\delta_0^{\alpha_{1,0}}(x_1)\dots\delta_{m-1}^{\alpha_{1,m-1}}(x_1)\dots\delta_0^{\alpha_{n,0}}(x_n)\dots\delta_{m-1}^{\alpha_{n,m-1}}(x_n)\qquad(5)$$

суммы принадлежит $[\Phi_{p^m}]$. Для этого заметим, что любую функцию вида (5) можно получить из функции

$$h=p^{m-1}a\delta_0(x_{1,0,0})\dots\delta_0(x_{1,p-1,0})\dots\delta_{m-1}(x_{1,1,m-1})\dots\delta_{m-1}(x_{1,p-1,m-1})\dots$$
$$\dots\delta_0(x_{n,0,0})\dots\delta_0(x_{n,p-1,0})\dots\delta_{m-1}(x_{n,0,m-1})\dots\delta_{m-1}(x_{n,p-1,m-1})$$

с помощью подходящего отождествления части ее переменных и подстановки вместо оставшихся переменных константы $(p^m-1)/(p-1)$.

Построение функции h производится в несколько этапов:

а) построение функций $p^i\delta_i(x_1)\ldots\delta_i(x_{t_i})$, $i\in\{0, 1, \ldots, m-1\}$,— с помощью подстановки функции $p^i\delta_i(x)\,\delta_i(y)$ в себя достаточное число раз;

б) построение функций $p^{m-1}\delta_i(x_1)\ldots\delta_i(x_{t_i})$, $i\in\{0, 1, \ldots, m-2\}$,— с помощью функции $x+y$ и функций, полученных на этапе а);

в) построение функции h — с помощью подстановки функций, полученных на этапе б), в функцию $p^{m-1}\delta_{m-1}(x_1)\ldots\delta_{m-1}(x_{t_{m-1}})$, построенную на этапе а).

Таким образом, $h\in[\Phi_{p^m}]$, и, следовательно, функции $p^{m-1}g(x_1, \ldots, x_n)$ и $f(x_1, \ldots, x_n)$ принадлежат классу $[\Phi_{p^m}]$. Тем самым доказана полнота системы функций Φ_{p^m} в $\mathfrak{M}_{p^m}$. Доказательство неприводимости этой системы проводится методом от противного индукцией по рангу формулы, представляющей функцию из системы Φ_{p^m}. Техника этого доказательства во многом повторяется в лемме 3 и здесь опущена ввиду того, что неприводимость системы Φ_{p^m} не используется в дальнейших рассмотрениях.

В заключение параграфа приведем некоторые наиболее часто используемые свойства координат p^m-значных функций, принадлежащих классу $\mathfrak{M}_{p^m}$.

Свойства координатных функций:

1. Функция $\delta_0(x)$ принадлежит классу $\mathcal{P}_{p^m}$. Этот факт непосредственно следует из критерия полиномиальности одноместных p^m-значных функций, доказанного в работе [15]. Например, при $p=2$ выполнено равенство $\delta_0(x)=x^{p^m-1}$ (при $p>2$ полиномиальное представление функции $\delta_0(x)$ не столь просто).

2. При $k=p^2$ функция $p\delta_1(x)$ принадлежит классу $\mathcal{P}_{p^2}$. Это следует из равенства $p\delta_1(x)=x-\delta_0(x)$ и свойства 1.

3. Если $f(x_1, \ldots, x_n)\in\mathfrak{M}_{p^m}$, то функция $\delta_0(f)$ принадлежит классу $\mathcal{P}_{p^m}$. По теореме 1 функция $\delta_0(f)$ представлена полиномом по модулю p от переменных $\delta_0(x_1), \ldots, \delta_0(x_n)$.

Осталось заметить, что операции сложения и умножения по модулю p нулевых компонент переменных суть полиномы из $\mathcal{P}_{p^m}$:

$$\delta_0(x)\oplus\delta_0(y)=\delta_0(x+y),$$
$$\delta_0(x)\cdot\delta_0(y)=\delta_0(x\cdot y),$$

а функции $\delta_0(x_1), \ldots, \delta_0(x_n)$ принадлежат $\mathcal{P}_{p^m}$ по свойству 1.

4. Координатные функции арифметических операций кольца $\mathbf{Z}_{p^m}$ имеют следующий вид:

$$\delta_i(x+y)=\delta_i(x)\oplus\delta_i(y)\oplus Q_1(\delta_0(x), \ldots, \delta_{i-1}(x), \delta_0(y), \ldots, \delta_{i-1}(y)),$$

$$\delta_i(x\cdot y)=\sum_{j=0}^{i}\delta_j(x)\,\delta_{i-j}(y)\oplus Q_2(\delta_0(x), \ldots, \delta_{i-1}(x), \delta_0(y), \ldots, \delta_{i-1}(y)),$$

где Q_1, Q_2 — подходящие полиномы над $\mathbf{Z}_p$, степени которых не превосходят $2i(p-1)$.

В дальнейшем нам потребуется еще одно понятие, связанное с координатными функциями. Возьмем произвольную функцию $f(x_1, \ldots, x_n)\in P_{p^m}$. Можно указать полиномиальное представление любой ее координаты $\delta_i(f)$:

$$\delta_i(f)=\sum_{\alpha_{1,0},\ldots,\alpha_{n,m-1}=0}^{p-1}a_{\alpha_{1,0},\ldots,\alpha_{n,m-1}}\delta_0^{\alpha_{1,0}}(x_1)\ldots\delta_{m-1}^{\alpha_{1,m-1}}(x_1)\ldots\delta_{m-1}^{\alpha_{n,m-1}}(x_n).$$

Определение 4. *Индексом одночлена*

$$R=a\delta_0^{\alpha_{1,0}}(x_1)\ldots\delta_{m-1}^{\alpha_{1,m-1}}(x_1)\ldots\delta_0^{\alpha_{n,0}}(x_n)\ldots\delta_{m-1}^{\alpha_{n,m-1}}(x_n),\qquad a\neq 0,$$

назовем целое число $\operatorname{ind}(R)$, равное $\sum_{i=1}^{n}\sum_{j=1}^{m-1} j\alpha_{i,j}$. *Индексом координатной функции* $\delta_i(f)$ назовем наибольший из индексов ненулевых одночленов в ее приведенном полиномиальном представлении по модулю p.

Непосредственно из определения индекса имеем еще одно свойство координатных функций.

5. Если $f(x_1, \ldots, x_n) \in \mathfrak{M}_{p^m}$, то

$$\operatorname{ind}(\delta_i(f)) \leqslant \sum_{j=1}^{n}\sum_{l=1}^{i}(p-1)\,l = (p-1)\,n\,\frac{i(i+1)}{2}.$$

В частности,

$$\operatorname{ind}(\delta_0(f)) = 0.$$

§ 2. Описание решетки, случай $k = p_1^2 \ldots p_s^2 p_{s+1} \ldots p_l$

В этом параграфе мы получим полное описание решетки $[\mathcal{P}_k;\ \mathfrak{M}_k]$ замкнутых классов, лежащих между $\mathcal{P}_k$ и $\mathfrak{M}_k$, в случае $k = p_1^2 \ldots p_s^2 p_{s+1} \ldots p_l$, где $p_1, \ldots, p_l$—различные простые числа.

Из теоремы 2 следует, что для решения этой задачи требуется описание решеток $\left[\mathcal{P}_{p_i^{\alpha_i}};\ \mathfrak{M}_{p_i^{\alpha_i}}\right]$, $i \in \{1, \ldots, l\}$. В нашем случае при $i \in \{s+1, \ldots, l\}$ $\mathcal{P}_{p_i} = \mathfrak{M}_{p_i}$. Поэтому остается выяснить структуру интервалов $[\mathcal{P}_{p_i^2};\ \mathfrak{M}_{p_i^2}]$, $i \in \{1, \ldots, s\}$.

С целью упрощения рассуждений в настоящем параграфе мы будем использовать понятие полиномиальной эквивалентности и полиномиальной сводимости.

Определение 5. Функции f и g называются *полиномиально эквивалентными*, если

$$f+g \in \mathcal{P}_k \quad \text{или} \quad f-g \in \mathcal{P}_k.$$

Функция g *полиномиально выводима* из функции f (или f *полиномиально сводима* к функции g), если существуют полиномы $h_0, h_1, \ldots, h_n \in \mathcal{P}_k$ такие, что

$$g = h_0(f(h_1, \ldots, h_n)).$$

Нетрудно проверить, что из полиномиальной эквивалентности функций f и g следует $[f, \mathcal{P}_k] = [g, \mathcal{P}_k]$, а из полиномиальной сводимости функции f к функции g—включение $[g, \mathcal{P}_k] \subseteq [f, \mathcal{P}_k]$.

Нам потребуется также критерий полиномиальности над кольцом $\mathbf{Z}_{p^2}$.

Утверждение 1. *Функция* $f \in P_{p^2}$ *является полиномом по модулю* p^2 *тогда и только тогда, когда выполнены условия*

$$\operatorname{ind}(\delta_0(f)) = 0, \quad \operatorname{ind}(\delta_1(f)) \leqslant 1. \tag{6}$$

Доказательство. Пусть $f \in \mathcal{P}_{p^2}$. Тогда на основании теоремы 1 функция $\delta_0(f)$ зависит лишь от нулевых координат переменных. Следовательно, $\operatorname{ind}(\delta_0(f)) = 0$. Неравенство $\operatorname{ind}(\delta_1(f)) \leqslant 1$ докажем индукцией по рангу формулы над $\{\mathbf{1}, x+y, x\cdot y\}$, представляющей функцию f.

Если f—переменная, то неравенство $\operatorname{ind}(\delta_1(f)) \leqslant 1$ является очевидным. Пусть теперь $f = R_1 + R_2$ или $f = R_1 \cdot R_2$, где R_1, R_2—формулы меньшего ранга. Тогда в первом случае

$$\delta_1(f) = \delta_1(R_1) \oplus \delta_1(R_2) \oplus Q_1(\delta_0(R_1),\ \delta_0(R_2)),$$

где Q_1—подходящий полином по модулю p, а во втором случае

$$\delta_1(f) = \delta_1(R_1)\,\delta_0(R_2) \oplus \delta_0(R_1)\,\delta_1(R_2) \oplus Q_2(\delta_0(R_1),\ \delta_0(R_2)),$$

где Q_2—также полином по модулю p.

По доказанному выше $\operatorname{ind}(\delta_0(R_1)) = \operatorname{ind}(\delta_0(R_2)) = 0$, а по предположению индукции $\operatorname{ind}(\delta_1(R_1)) \leqslant 1$, $\operatorname{ind}(\delta_1(R_2)) \leqslant 1$. Следовательно, в первом случае

$$\operatorname{ind}(\delta_1(f)) = \max\{\operatorname{ind}(\delta_1(R_1)), \quad \operatorname{ind}(\delta_1(R_2)), \quad \operatorname{ind}(Q_1)\} \leqslant \max\{1, \ 1, \ 0\} = 1,$$

а во втором случае

$$\operatorname{ind}(\delta_1(f)) = \max\{\operatorname{ind}(\delta_1(R_1)\,\delta_0(R_2)), \ \operatorname{ind}(\delta_0(R_1)\,\delta_1(R_2)), \ \operatorname{ind}(Q_2)\} \leqslant$$
$$\leqslant \max\{\operatorname{ind}(\delta_1(R_1)) + \operatorname{ind}(\delta_0(R_2)),$$
$$\operatorname{ind}(\delta_0(R_1)) + \operatorname{ind}(\delta_1(R_2)), \ \operatorname{ind}(Q_2)\} \leqslant \max\{1, \ 1, \ 0\} = 1.$$

Обратно, пусть выполнено условие (6). Тогда по свойству 3 координатных функций функция $\delta_0(f)$ является полиномом. Если теперь установить включение $p\delta_1(f) \in \mathcal{P}_{p^2}$, то будем иметь $f \in \mathcal{P}_{p^2}$.

Так как по условию $\operatorname{ind}(\delta_1(f)) \leqslant 1$, то

$$p\delta_1(f) = p\sum_{i=1}^{n} a_i\delta_1(x_i)\,F_i(\delta_0(x_1), \ldots, \delta_0(x_n)) = p\sum_{i=1}^{n} a_i\delta_1(x_i)F_i(\delta_0(x_1), \ldots, \delta_0(x_n)),$$

где в последней сумме арифметические операции уже из кольца $\mathbf{Z}_{p^2}$. Так как $F_i(\delta_0(x_1), \ldots, \delta_0(x_n)) = \delta_0(F_i(\delta_0(x_1), \ldots, \delta_0(x_n)))$, то по свойству 3 координатных функций заключаем, что $F_i \in \mathcal{P}_{p^2}$ $(i \in \{1, \ldots, n\})$. Осталось заметить, что по свойству 2 функции $p\delta_1(x_i) = x_i - \delta_0(x_i)$ $(i \in \{1, \ldots, n\})$, являются полиномами из $\mathcal{P}_{p^2}$. Таким образом, функция f принадлежит классу $\mathcal{P}_{p^2}$, и утверждение доказано полностью.

Приведенное далее утверждение было анонсировано ранее в работе [5].

Лемма 2. *Пусть p — простое число. Тогда класс $\mathcal{P}_{p^2}$ предполон в $\mathfrak{M}_{p^2}$.*

Доказательство. Возьмем произвольную функцию $f(x_1, \ldots, x_n) \in \mathfrak{M}_{p^2} \setminus \mathcal{P}_{p^2}$ и покажем, что функция $p\delta_1(x)\,\delta_1(y)$ принадлежит классу $[f, \mathcal{P}_{p^2}]$. Тогда с учетом того, что функция $\delta_0(x)\,\delta_0(y)$ является полиномом из $\mathcal{P}_{p^2}$, по теореме 3 получим $[f, \mathcal{P}_{p^2}] = \mathfrak{M}_{p^2}$.

Без ограничения общности можно считать, что $\delta_0(f) = 0$. Действительно, так как по свойству 3 $\delta_0(f) \in \mathcal{P}_{p^2}$, то функции $f(x_1, \ldots, x_n)$ и $p\delta_1(f)$ полиномиально эквивалентны.

Так как $f(x_1, \ldots, x_n) \notin \mathcal{P}_{p^2}$, то по предыдущему утверждению $\operatorname{ind}(\delta_1(f)) > 1$. Тогда имеет место один из следующих двух случаев.

1. Существуют $i \in \{1, \ldots, n\}$ и $\beta \in \{2, \ldots, p-1\}$ такие, что

$$f = p\delta_1(f) = p\sum_{\alpha=2}^{p-1} \delta_1^{\alpha}(x_i)\,F_{\alpha,\,i}(\delta_0(x_i), \ x_1, \ \ldots, \ x_{i-1}, \ x_{i+1}, \ \ldots, \ x_n) +$$
$$+ p\delta_1(x_i)\,F_{1,\,i}(\delta_0(x_i), \ x_1, \ \ldots, \ x_{i-1}, \ x_{i+1}, \ \ldots, \ x_n) +$$
$$+ pF_{0,\,i}(\delta_0(x_i), \ x_1, \ \ldots, \ x_{i-1}, \ x_{i+1}, \ \ldots, \ x_n),$$

где $F_{\beta,\,i} \not\equiv 0$.

2. Существуют $i, \ j \in \{1, \ldots, n\}$, $i \neq j$, такие, что

$$f = p\delta_1(f) =$$
$$= p\delta_1(x_i)\,\delta_1(x_j)\,F_{i,\,j}(\delta_0(x_i), \delta_0(x_j), x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n) +$$
$$+ p\delta_1(x_i)\,F_i(\delta_0(x_i), \delta_0(x_j), x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n) +$$
$$+ p\delta_1(x_j)\,F_j(\delta_0(x_i), \delta_0(x_j), x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n) +$$
$$+ pF(\delta_0(x_i), \delta_0(x_j), x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n),$$

где $F_{i,\,j} \not\equiv 0$.

Отметим, что случай 1 возможен лишь при $p > 2$. Разбор ситуаций начнем со случая 2.

Так как $F_{i,\,j} \not\equiv 0$, то найдутся константы $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_{j-1}, a_{j+1}, \ldots, a_n \in \Omega_{p^2}$ и $b_i, \ b_j \in \Omega_p$ такие, что

$$F_{i,\,j}(b_i, \ b_j, \ a_1, \ \ldots, \ a_{i-1}, \ a_{i+1}, \ \ldots, \ a_{j-1}, \ a_{j+1}, \ \ldots, \ a_n) = c, \qquad c \neq 0.$$

Зафиксируем переменные x_t константами a_t, $t \in \{1, \ldots, n\} \setminus \{i, j\}$, а вместо x_i и x_j подставим полиномы $b_i + p\delta_1(x_i)$ и $b_j + p\delta_1(x_j)$ соответственно. Учитывая, что функция вида $pa\delta_1(x)$—полином, заключаем, что f полиномиально сводима к функции

$$h(x, y) = pc\delta_1(x)\,\delta_1(y).$$

Умножая полученную функцию на c^{-1} (элемент $c \in \Omega_p \setminus \{0\}$ обратим в кольце $\mathbf{Z}_{p^2}$), получаем

$$p\delta_1(x)\,\delta_1(y) \in [f, \mathcal{P}_{p^2}].$$

Рассмотрим теперь случай 1. Так как $F_{\beta, i} \not\equiv 0$, то, как и раньше, с помощью фиксации переменных $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ подходящими константами и подстановки вместо x_i полинома вида $b + p\delta_1(x)$, $b \in \Omega_p$, полиномиально сводим функцию f к функции вида

$$g(x) = p \sum_{\alpha=2}^{p-1} d_\alpha \delta_1^\alpha(x).$$

Пусть $\hat{\alpha} = \max\{\alpha \mid d_\alpha \not\equiv 0\}$. Тогда $2 \leqslant \hat{\alpha} \leqslant p-1$ и $\operatorname{ind}(\delta_1(g)) = \hat{\alpha}$. Укажем теперь последовательность функций $g_0(x), \ldots, g_{\hat{\alpha}-2}(x)$ такую, что:

а) $g_0(x) = g(x)$;

б) $g_{i+1} \in [g_i, \mathcal{P}_{p^2}]$, $i \in \{0, \ldots, \hat{\alpha}-3\}$;

в) $\operatorname{ind}(\delta_1(g_i)) = \hat{\alpha} - i$, $i \in \{0, \ldots, \hat{\alpha}-2\}$;

г) коэффициент при старшем члене $\delta_1^{\hat{\alpha}-i}(x)$ у функции $\delta_1(g_i)$ равен $d_{\hat{\alpha}}\hat{\alpha}(\hat{\alpha}-1)\ldots(\hat{\alpha}-i+1) \pmod p$.

Вначале заметим, что $\delta_1(p + p\delta_1(x)) = 1 \oplus \delta_1(x) \pmod p$. Поэтому, если функция $v(x)$ является полиномом от $\delta_1(x)$, то после подстановки в $v(x)$ вместо x функции $p + p\delta_1(x) \in \mathcal{P}_{p^2}$ получаем функцию $v(p + p\delta_1(x))$—полином от $\delta_1(x)$.

Теперь предположим, что функции $g_0(x), \ldots, g_i(x)$ с требуемыми свойствами уже построены. Построим функцию $g_{i+1}(x)$. Пусть

$$g_i(x) = p \sum_{\alpha=0}^{\hat{\alpha}-i} c_\alpha \delta_1^\alpha(x),$$

где по предположению индукции $c_{\hat{\alpha}-i} = d_{\hat{\alpha}}\hat{\alpha}(\hat{\alpha}-1)\ldots(\hat{\alpha}-i+1)$.

Положим $g_{i+1}(x) = g_i(p + p\delta_1(x)) - g_i(x) - g_i(p)$. Очевидно, $g_{i+1} \in [g_i, \mathcal{P}_{p^2}]$ и g_{i+1} представляет собой полином от $\delta_1(x)$. Выпишем этот полином:

$$g_{i+1}(x) = p \sum_{\alpha=0}^{\hat{\alpha}-i} c_\alpha \sum_{\beta=0}^{\alpha} \delta_1^\beta(x) \binom{\alpha}{\beta} - p \sum_{\alpha=0}^{\hat{\alpha}-i} c_\alpha \delta_1^\alpha(x) - p \sum_{\alpha=0}^{\hat{\alpha}-i} c_\alpha = p \sum_{\alpha=1}^{\hat{\alpha}-i} c_\alpha \sum_{\beta=1}^{\alpha-1} \delta_1^\beta(x) \binom{\alpha}{\beta}.$$

Коэффициент при старшем члене $\delta_1^{\hat{\alpha}-i-1}(x)$ у функции $g_{i+1}(x)$ равен $pc_{\hat{\alpha}-i}(\hat{\alpha}-i) = pd_{\hat{\alpha}}\hat{\alpha}\ldots(\hat{\alpha}-i)$ и отличен от нуля по модулю p^2 при $i < \hat{\alpha} \leqslant p-1$.

По определению индекса функции получаем $\operatorname{ind}(\delta_1(g_{i+1})) = \hat{\alpha} - i - 1$. По своему построению функция g_{i+1} принадлежит классу $[g_i, \mathcal{P}_{p^2}]$. Тем самым индукционный переход завершен.

Теперь рассмотрим функцию $g_{\hat{\alpha}-2}(x)$. Она имеет вид

$$g_{\hat{\alpha}-2}(x) = pd_{\hat{\alpha}}\hat{\alpha}(\hat{\alpha}-1)\ldots 3\delta_1^2(x) + pr_1\delta_1(x) + pr_0.$$

По свойству 2 функция $g_{\hat{\alpha}-2}$ эквивалентна функции

$$h_1(x) = pd_{\hat{\alpha}}\hat{\alpha}(\hat{\alpha}-1)\ldots 3\delta_1^2(x).$$

Из $h_1(x)$ с помощью умножения ее на константу $(d_{\hat{\alpha}}\hat{\alpha}(\hat{\alpha}-1)\ldots 3)^{-1}$ получаем функцию

$$h_2(x) = p\delta_1^2(x).$$

Осталось заметить, что

$$2p\delta_1(x)\,\delta_1(y) = h_2(p\delta_1(x)+p\delta_1(y)) - h_2(x) - h_2(y).$$

Поскольку $p>2$, то 2—обратимый элемент кольца $\mathbf{Z}_{p^2}$. Следовательно, функция $p\delta_1(x)\,\delta_1(y)$ принадлежит классу $[h_2, \mathcal{P}_{p^2}]$. Поскольку на каждом этапе мы получали функции, либо полиномиально эквивалентные исходной, либо полиномиально выводимые из нее, то $p\delta_1(x)\,\delta_1(y)\in[f, \mathcal{P}_{p^2}]$. Тем самым доказательство леммы полностью завершено.

Непосредственным следствием леммы 2 и теоремы 2 является

Теорема 4 [7]. *Пусть* $k = p_1^2\ldots p_s^2 p_{s+1}\ldots p_l$, *где* $p_1, \ldots, p_l$—*различные простые числа. Тогда решетка* $[\mathcal{P}_k; \mathfrak{M}_k]$ *изоморфна единичному* s*-мерному кубу.*

Согласно теореме 1, элементами решетки $[\mathcal{P}_k; \mathfrak{M}_k]$ являются замкнутые классы вида $\mathfrak{M}_k^{\mathfrak{A}_1,\ldots,\mathfrak{A}_l}$, где $\mathfrak{A}_i\in\left\{\mathcal{P}_{p_i^2}, \mathfrak{M}_{p_i^2}\right\}$ при $i\in\{1,\ldots,s\}$ и $\mathfrak{A}_j = \mathfrak{M}_{p_j}$ при $j\in\{s+1,\ldots,l\}$. Эти замкнутые классы удобно задавать в виде $\mathfrak{M}_k^{(\nu_1,\ldots,\nu_s)}$, где $\nu_i = 0$, если $\mathfrak{A}_i = \mathcal{P}_{p_i^2}$, и $\nu_i = 1$, если $\mathfrak{A}_i = \mathfrak{M}_{p_i^2}$, $i\in\{1,\ldots,s\}$. Тогда класс $\mathfrak{M}_k^{\tilde{\nu}}$ содержится в классе $\mathfrak{M}_k^{\tilde{\mu}}$ в том и только том случае, если $\tilde{\nu}\leqslant\tilde{\mu}$.

С помощью теоремы 4 несложно выводится

Утверждение 2. *Пусть* $k = p_1^2\ldots p_s^2 p_{s+1}\ldots p_l$ *и* $f\in\mathfrak{M}_k$. *Если среди классов* $\mathfrak{M}_k^{\tilde{\nu}}$, *содержащих* f, *класс* $\mathfrak{M}_k^{\tilde{\mu}}$ *является минимальным, то*

$$[f, \mathfrak{M}_k^{\tilde{\tau}}] = \mathfrak{M}_k^{\tilde{\mu}\vee\tilde{\tau}},$$

где $\tilde{\mu}\vee\tilde{\tau} = (\mu_1\vee\tau_1, \ldots, \mu_s\vee\tau_s)$. (*Здесь* $\vee$—*операция дизъюнкции.*)

Доказательство. По теореме 4 имеем $[f, \mathfrak{M}_k^{\tilde{\tau}}] = \mathfrak{M}_k^{\tilde{\lambda}}$. Так как по лемме 1 $\psi_{p_i^2}(\mathfrak{M}_k^{\tilde{\lambda}}) = [\psi_{p_i^2}(f), \psi_{p_i^2}(\mathfrak{M}_k^{\tilde{\tau}})]_{p_i^2}$, то при $\tau_i\geqslant\mu_i$ имеем $\psi_{p_i^2}(\mathfrak{M}_k^{\tilde{\lambda}}) = \psi_{p_i^2}(\mathfrak{M}_k^{\tilde{\tau}})$, а при $\tau_i<\mu_i$ по лемме 2 имеем $\psi_{p_i^2}(\mathfrak{M}_k^{\tilde{\lambda}}) = [\psi_{p_i^2}(f), \mathcal{P}_{p_i^2}] = \mathfrak{M}_{p_i^2}$. Следовательно, $\lambda_i = \mu_i\vee\tau_i$. Утверждение доказано.

§ 3. Бесконечность решетки, случай $k = p^3q$

В этом параграфе мы покажем, что при $k = p^3q$, $p>1$, $q\geqslant 1$ между классами $\mathcal{P}_k$ и $\mathfrak{M}_k$ существует бесконечная цепочка замкнутых классов. Ввиду теоремы 2 достаточно рассмотреть случай, когда $k = p^3$, где p—простое число. В этом случае определим систему функций

$$\mathcal{B}_{p^3}^{(s)} = \{1,\ x+y,\ x\cdot y,\ p^2\delta_1(x),\ \ldots,\ p^2\delta_1(x_1)\ldots\delta_1(x_s)\}$$

и рассмотрим ее замыкание $\mathfrak{B}_{p^3}^{(s)} = [\mathcal{B}_{p^3}^{(s)}]$.

Лемма 3. *При* $s\geqslant 2p-2$ *из* $f\in\mathfrak{B}_{p^3}^{(s)}$ *следует, что*

$$\operatorname{ind}(\delta_0(f)) = 0,\quad \operatorname{ind}(\delta_1(f))\leqslant 1,\quad \operatorname{ind}(\delta_2(f))\leqslant s. \tag{7}$$

Доказательство. Рассмотрим гомоморфизм ψ: $\mathfrak{M}_{p^3} \to \mathfrak{M}_{p^2}$, состоящий в приведении функции по модулю p^2. Поскольку функции $p^2\delta_1(x)$, ..., $p^2\delta_1(x_1)\ldots\delta_1(x_s)$ принадлежат ядру гомоморфизма ψ, то по лемме 1 имеем $\psi(\mathfrak{B}_{p^3}^{(s)}) = [\psi(\mathcal{B}_{p^3}^{(s)})]_{p^2} = \mathcal{P}_{p^2}$.

Следовательно, если $f \in \mathfrak{B}_{p^3}^{(s)}$, то функция $\psi(f) = \delta_0(f) + p\delta_1(f)$ принадлежит классу $\mathcal{P}_{p^2}$. По утверждению 1 заключаем, что

$$\operatorname{ind}(\delta_0(f)) = 0, \quad \operatorname{ind}(\delta_1(f)) \leqslant 1.$$

Последнее неравенство из (7) будем доказывать индукцией по рангу r формулы, представляющей функцию $f \in \mathfrak{B}_{p^3}^{(s)}$. Пусть $r = 0$. Для селекторов (переменных) неравенства (7) выполнены.

Предполагая справедливость неравенств (7) для всех функций из $\mathfrak{B}_{p^3}^{(s)}$, представимых формулами ранга, не превосходящего $l-1$, докажем неравенства (7) для формул ранга $r = l$. Возможны следующие ситуации:

а) $f = \mathbf{1}$;

б) $f = R_1 + R_2$, где $\operatorname{rang} R_1 \leqslant l-1$, $\operatorname{rang} R_2 \leqslant l-1$;

в) $f = R_1 \cdot R_2$, где $\operatorname{rang} R_1 \leqslant l-1$, $\operatorname{rang} R_2 \leqslant l-1$;

г) $f = p^2\delta_1(R_1)\ldots\delta_1(R_j)$, где $\operatorname{rang}(R_j) \leqslant l-1$, $j \in \{1, \ldots, s\}$.

В случае а) $\operatorname{ind}(\delta_2(f)) = 0$.

В случае б)

$$\delta_2(f) = \delta_2(R_1) \oplus \delta_2(R_2) \oplus Q_1(\delta_0(R_1), \delta_1(R_1), \delta_0(R_2), \delta_1(R_2)),$$

где Q_1 — приведенный полином по модулю p от $\delta_0(R_1)$, $\delta_1(R_1)$, $\delta_0(R_2)$, $\delta_1(R_2)$. По доказанному выше $\operatorname{ind}(\delta_0(R_i)) = 0$, $\operatorname{ind}(\delta_1(R_i)) \leqslant 1$ при $i \in \{1, 2\}$. Следовательно,

$$\operatorname{ind}(Q_1(\delta_0(R_1), \delta_1(R_1), \delta_0(R_2), \delta_1(R_2))) \leqslant 2p-2 \leqslant s.$$

Используя предположение индукции $\operatorname{ind}(\delta_2(R_i)) \leqslant s$, $i \in \{1, 2\}$, получаем

$$\operatorname{ind}(\delta_2(f)) \leqslant \max\{\operatorname{ind}(\delta_2(R_1)), \operatorname{ind}(\delta_2(R_2)), \operatorname{ind}(Q_1)\} \leqslant s.$$

В случае в)

$$\delta_2(f) = \delta_2(R_1)\,\delta_0(R_2) \oplus \delta_0(R_1)\,\delta_2(R_2) \oplus \delta_1(R_1)\,\delta_1(R_2) \oplus Q_2(\delta_0(R_1), \delta_1(R_1), \delta_0(R_2), \delta_1(R_2)).$$

Так как $\operatorname{ind}(\delta_0(R_i)) = 0$, $\operatorname{ind}(\delta_1(R_i)) \leqslant 1$, $\operatorname{ind}(\delta_2(R_i)) \leqslant s$, $i \in \{1, 2\}$, то так же, как и выше, получаем неравенство

$$\operatorname{ind}(\delta_2(f)) \leqslant \max\{s, s, 2, 2p-2\} \leqslant s.$$

Наконец, в случае г) из $\operatorname{ind}(\delta_1(R_j)) \leqslant 1$ следует

$$\operatorname{ind}(\delta_2(p^2\delta_1(R_1)\ldots\delta_1(R_j))) = \operatorname{ind}(\delta_1(R_1)\ldots\delta_1(R_j)) \leqslant j \leqslant s.$$

Утверждение доказано полностью.

Теорема 5. *Если $k = p^3q$, где $p > 1$ — простое число, то между $\mathcal{P}_k$ и $\mathfrak{M}_k$ существует бесконечная цепочка замкнутых классов*

$$\mathcal{P}_k \subseteq \mathfrak{B}_k^{(2p-1)} \subseteq \mathfrak{B}_k^{(2p)} \subseteq \ldots \subseteq \bigcup_{s=2p-1}^{\infty} \mathfrak{B}_k^{(s)} \subseteq \mathfrak{M}_k,$$

где $\mathfrak{B}_k^{(s)}$ — прообраз замкнутого класса $\mathfrak{B}_{p^3}^{(s)}$ при естественном гомоморфизме $\mathfrak{M}_{p^3q} \to \mathfrak{M}_{p^3}$.

Доказательство. Достаточно показать, что при любом $s \geqslant 2p-1$ выполнено строгое включение $\mathfrak{B}_{p^3}^{(s)} \subsetneq \mathfrak{B}_{p^3}^{(s+1)}$. По построению $\mathfrak{B}_{p^3}^{(s)} \subseteq \mathfrak{B}_{p^3}^{(s+1)}$. Из утверждения 2 следует, что функция $p^2\delta_1(x_1)\ldots\delta_1(x_{s+1})$ не принадлежит классу $\mathfrak{B}_{p^3}^{(s)}$, поскольку $\operatorname{ind}(\delta_2(p^2\delta_1(x_1)\ldots\delta_1(x_{s+1}))) = s+1$. Таким образом, $\mathfrak{B}_{p^3}^{(s)} \neq \mathfrak{B}_{p^3}^{(s+1)}$.

Наконец, включение $\bigcup_{s=2p-1}^{\infty} \mathfrak{B}_k^{(s)} \subseteq \mathfrak{M}_k$ строгое, поскольку замкнутый класс $\bigcup_{s=2p-1}^{\infty} \mathfrak{B}_k^{(s)}$ не имеет конечного базиса (как объединение строго возрастающей цепочки замкнутых классов [13]), а класс $\mathfrak{M}_k$ конечно порожден, что следует, например, из теорем 3 и 2.

Объяснить эффект наличия бесконечной цепочки от $\mathcal{P}_k$ до $\mathfrak{M}_k$ при k, не свободном от кубов целых чисел, можно, по-видимому, различием свойств колец $\mathbf{Z}_{p^2}$ и $\mathbf{Z}_{p^3}$. Например, при $k=4$ группа аффинных преобразований кольца $\mathbf{Z}_4$ является максимальной подгруппой симметрической группы S_4, а при $k=8$ это утверждение неверно.

В заключение отметим, что вопрос о счетности или континуальности решетки $[\mathcal{P}_k; \mathfrak{M}_k]$ остается пока открытым так же, как и вопрос о построении цепочек замкнутых классов от $\bigcup_{s=2p-1}^{\infty} \mathfrak{B}_k^{(s)}$ до $\mathfrak{M}_k$.

СПИСОК ЛИТЕРАТУРЫ

1. Айзенберг Н. Н., Семйон И. В. Некоторые критерии представимости функций k-значной логики полиномами по модулю k // Многоустойчивые элементы и их применения.— М.: Сов. радио, 1971.— С. 84—88.
2. Виноградов И. М. Основы теории чисел.— М.: Наука, 1981.—176 с.
3. Мальцев А. И. Итеративные алгебры Поста.— Новосибирск: Изд-во НГУ, 1958.—101 с.
4. Марченков С. С., Деметрович Я., Ханнак Л. О замкнутых классах самодвойственных функций в P_3 // Методы дискретного анализа в решении комбинаторных задач. Вып. 34.— Новосибирск, 1980.— С. 38—73.
5. Мещанинов Д. Г. Квазиполиномиальные классы k-значных логик // Прикладная математика и математическое обеспечение ЭВМ.— М.: Изд-во МГУ, 1985.— С. 52—53.
6. Мещанинов Д. Г. О надструктуре класса полиномов в P_k // VII Всесоюзная конференция «Проблемы теоретической кибернетики». 18—20 сентября 1985. Тезисы докладов. Ч. 1.— Иркутск, 1985.—135 с.
7. Мещанинов Д. Г. О полиномиальной реализации функций k-значной логики / ВИНИТИ.— М., 1987.— Деп. в ВИНИТИ 23.10.87, № 7441-887.
8. Нечаев А. А. Критерий полноты систем функций p^n-значной логики, содержащий операции сложения и умножения по модулю p^n // Методы дискретного анализа в решении комбинаторных задач. Вып. 34.— Новосибирск, 1980.— С. 74—89.
9. Ремизов А. Б. Критерий линеризуемости конечных колец // VII Всесоюзная конференция по теории колец, алгебр и модулей. Тезисы докладов.— Новосибирск, 1983.— С. 101.
10. Черепов А. Н. Описание надструктуры класса полиномов в P_k ($k=p^m$) // Некоторые вопросы прикладной математики и программного обеспечения ЭВМ.— М.: Изд-во МГУ, 1982.— С. 97—98.
11. Черепов А. Н. Описание структуры замкнутых классов в P_k, содержащих класс полиномов // Проблемы кибернетики. Вып. 40.— М.: Наука, 1983.— С. 5—18.
12. Черепов А. Н. Надструктура класса сохранения отношений сравнения в многозначной логике // XII Всесоюзная конференция «Проблемы теоретической кибернетики». 18—20 сентября 1985. Тезисы докладов. Ч. 1.— Иркутск, 1985.— С. 200—201.
13. Яблонский С. В. Функциональные построения в k-значной логике // Труды МИ АН СССР.— 1958.— Т. 51.— С. 5—142.
14. Янов Ю. И., Мучник А. А. О существовании k-значных замкнутых классов, не имеющих конечного базиса // ДАН СССР.—1959.— Т. 127, № 1.— С. 44—46.
15. Carlitz L. Functions and polinomials (mod p^n) // Acta Arithm.—1964.— № 9.— P. 66—78.
16. Rosenberg I. G. La structure der fonctions de plusieurs variables sur un ensemble fini // C. R. Acad. Sci. Paris, Ser. A. B. 260.—1965.— P. 3817—3819.
17. Rosenberg I. G. Completeness properties of multiple-valued logic algebras // Computer science and multiple-valued logic. Theory and applications/Ed. D. Rine).— Amsterdam: North Holland, 1977.
18. Szendrei A. On closed sets of linear operations over finite sets of square—free cardinality // Electron. Inform. Verarb. und Kibern.—1978.— V. 14, № 11.— P. 547—559.

Статья поступила 19.05.88