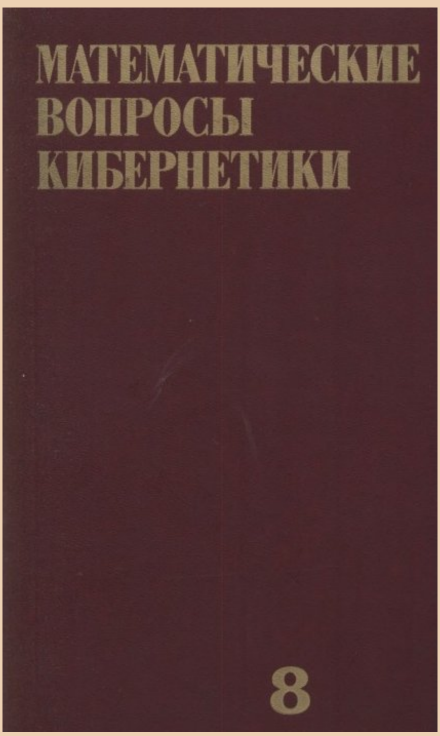


Д. Г. Мещанинов

О замкнутых классах k-значных функций, сохраняющих первые d-разности

О ЗАМКНУТЫХ КЛАССАХ k-ЗНАЧНЫХ ФУНКЦИЙ, СОХРАНЯЮЩИХ ПЕРВЫЕ d-РАЗНОСТИ

Д. Г. МЕЩАНИНОВ

(МОСКВА)

Пусть k — натуральное число, $k \geqslant 2$, $E_k = \{0, 1, \ldots, k-1\}$, $P_k = \{f\colon E_k^n \to E_k,\ n = 0, 1, \ldots\}$ — класс всех функций k-значной логики. Рассмотрим алгебру P_k с операциями суперпозиции, называемую функциональной системой, и ее подалгебры, называемые замкнутыми классами. Известно, что при $k \geqslant 3$ множество всех замкнутых классов в P_k имеет мощность континуум [16] и потому является труднообозримым. Один из путей преодоления этой трудности состоит в выделении некоторых семейств классов, допускающих лаконичное описание и позволяющих выяснить их структуру. В связи с таким подходом внимание ряда исследователей в 80–90-е годы привлекли семейства классов, содержащих полиномы по составному модулю k [2, 3, 5–14]. Известно, что при составном k функции, представимые полиномами (в дальнейшем будем рассматривать только полиномы по модулю k), образуют собственный замкнутый подкласс Pol в P_k, а при простом k имеет место равенство $\mathrm{Pol} = P_k$. Анализ условий, являющихся необходимыми или достаточными для представимости k-значных функций полиномами, привел к выделению, в частности, двух свойств функций: сохранению сравнений по модулям d и сохранению конечных разностей, вычисленных с шагами d, где d — это делители числа k. Эти свойства определяют два семейства классов $C(d)$ и $R(d)$ соответственно (точные определения будут даны ниже). Структура замкнутых классов функций, сохраняющих сравнения по одному или нескольким модулям-делителям числа k, полностью описана А. Н. Череповым [13, 14]. В общем случае она имеет достаточно сложный вид, но конечна; в частных случаях $k = p_1^m$ и $k = p_1 \ldots p_s$, где $p_1, \ldots, p_s$ — это различные простые числа, она упрощается. Так, при $k = p_1^m$ эта решетка изоморфна $(m-1)$-мерному единичному кубу. Позднее были получены результаты о структуре классов, находящихся между классами Pol и $M(k)$, где $M(k)$ — это класс функций, сохраняющих сравнения по всем модулям-делителям числа k [2, 3, 7, 8, 10–12], о структуре подклассов в Pol, содержащих все линейные функции [5], о решетке классов $R(d)$ [11]. Было, в частности, выяснено, что для любого собственного делителя d числа k имеет место включение $R(d) \subset C(d)$ и справедливо равенство $R(k) = C(k) = P_k$. В статье [11] введено также семейство классов $L(d)$, которые содержатся в $R(d)$. Классы $R(d)$ образуют решетку, изоморфную решетке делителей числа k; такую же решетку образуют классы $L(d)$. В настоящей работе мы анализируем классы $R(d)$, $L(d)$, а также $R(d_1) \cap C(d_2)$ (d_1 и d_2 — это взаимно простые делители числа k). Выявленные свойства таких классов позволили построить решетку подклассов класса Pol в $p_1 \ldots p_s$-значной логике, содержащих все линейные функции (здесь $p_1, \ldots, p_s$ — различные простые числа). Оказалось, что эта решетка изоморфна s-мерному единичному кубу. Заметим, что решетка таких классов в 4-значной логике, построенная А. А. Крохиным, К. Л. Сафиным и Е. В. Сухановым [5], намного сложнее и даже бесконечна.

Будем применять следующие обозначения: $\widetilde{x} = (x_1, \ldots, x_n)$, $\widetilde{0} = (0, \ldots \ldots, 0)$ — n-мерные векторы; $[\{f_1, \ldots, f_m\}]$ — замыкание относительно суперпозиции системы функций $\{f_1, \ldots, f_m\}$; $+, -, \cdot$ — операции кольца вычетов по модулю k; $(a, b, \ldots, c)$ — наибольший общий делитель натуральных чисел $a, b, \ldots, c$. Буквами p (возможно, с индексами) будут обозначаться простые числа. Запись $\widetilde{\alpha} \equiv \widetilde{\beta} \pmod d$ означает, что для всех i, $i = 1, \ldots, n$, выполняются сравнения $\alpha_i \equiv \beta_i \pmod d$. Запись $d|e$ означает, что натуральное число d делит число e.

Введем основные замкнутые классы, которые будут рассматриваться в работе. Если $d|k$, то $C(d)$ — *замкнутый класс функций, сохраняющих сравнение по модулю* d, т. е. удовлетворяющих условию

$$\widetilde{\alpha} \equiv \widetilde{\beta} \pmod d \Rightarrow f(\widetilde{\alpha}) \equiv f(\widetilde{\beta}) \pmod d.$$

Если $d_1, \ldots, d_r$ — различные делители числа k, то $C(d_1, \ldots, d_r) = C(d_1) \cap \ldots \ldots \cap C(d_r)$. Далее, если $d|k$, то

$$M(d) = \bigcap_{e|d} C(e).$$

Пусть $d|k$. Величины

$$\Delta_i f(\widetilde{x}) = f(x_1, \ldots, x_{i-1}, x_i + d, x_{i+1}, \ldots, x_n) - f(\widetilde{x})$$

называются *(первыми) d-разностями функции f по переменной x_i*, вычисленными *в точке $\widetilde{x}$*. Через $R(d)$ (через $L(d)$) обозначаем *замкнутый класс функций, сохраняющих (абсолютно сохраняющих) d-разности*, т. е. удовлетворяющих условию: для всех i, $i = 1, \ldots, n$, всех $\widetilde{\mu}$ из E_d^n и всех таких векторов $\widetilde{x}$, что $\widetilde{x} \equiv \widetilde{\mu} \pmod d$, разности $\Delta_i f(\widetilde{x})$ зависят только от i и $\widetilde{\mu}$ (зависят только от i). *Класс всех линейных функций* будем обозначать как L. Заметим, что имеют место равенства $L = L(1) = R(1)$.

Будем также использовать функции

$$g_d(\widetilde{x}) = \begin{cases} 1, & \widetilde{x} \equiv \widetilde{0} \pmod d, \\ 0, & \widetilde{x} \not\equiv \widetilde{0} \pmod d, \end{cases} \qquad \psi_d(\widetilde{x}) = \begin{cases} d, & \widetilde{x} = \widetilde{0}, \\ 0, & \widetilde{x} \neq \widetilde{0}. \end{cases}$$

§ 1. Периодические функции

Напомним, что функция $f(\widetilde{x})$, удовлетворяющая условию

$$\widetilde{\alpha} \equiv \widetilde{\beta} \pmod d \Rightarrow f(\widetilde{\alpha}) = f(\widetilde{\beta}),$$

называется *d-периодической* (при этом предполагается, что $d|k$). В данном параграфе мы выведем некоторые вспомогательные результаты о периодических функциях.

Лемма 1. *Если d_0, d_1, d_2 — делители числа k, и $d_0 = (d_1, d_2)$, то d_1-периодическая функция $f(\widetilde{x})$ принадлежит классу $C(d_2)$ в том и только том случае, когда она удовлетворяет условию*

$$\widetilde{\alpha} \equiv \widetilde{\beta} \pmod{d_0} \Rightarrow f(\widetilde{\alpha}) \equiv f(\widetilde{\beta}) \pmod{d_2}. \tag{1}$$

Доказательство. Достаточность условия (1) для сохранения функцией сравнения по модулю d_2 очевидна. Докажем необходимость.

Пусть $\widetilde{\alpha} \equiv \widetilde{\beta} \pmod{d_0}$, т. е. $\widetilde{\beta} - \widetilde{\alpha} = \widetilde{\gamma} d_0$. Числа d_1, d_2 и k можно представить в виде $d_1 = a d_0$, $d_2 = b d_0$, $k = abc d_0$, причем $(a, b) = 1$. Тогда найдутся такие целочисленные векторы $\widetilde{A}$ и $\widetilde{B}$, что $\widetilde{\gamma} = \widetilde{A} a + \widetilde{B} b$. Умножив это равенство на d_0, получим $\widetilde{\beta} - \widetilde{\alpha} = \widetilde{A} d_1 + \widetilde{B} d_2$. В силу d_1-периодичности функции имеем: $f(\widetilde{\beta}) = f(\widetilde{\alpha} + \widetilde{A} d_1 + \widetilde{B} d_2) = f(\widetilde{\alpha} + \widetilde{B} d_2)$. Далее, из условия $f \in C(d_2)$ следует, что $f(\widetilde{\alpha} + \widetilde{B} d_2) \equiv f(\widetilde{\alpha}) \pmod{d_2}$. Таким образом, выполнимость условия (1) доказана.

Следствие 1. *Если d_1 и d_2 — взаимно простые делители числа k, то d_1-периодическая функция принадлежит классу $C(d_2)$ в том и только том случае, когда все ее значения сравнимы между собой по модулю d_2.*

Интересно сопоставить этот результат со следующим фактом, объединяющим два утверждения статьи [11] — лемму 17 и теорему 5.

Лемма 2. *Если d_0, d_1, d_2 — делители числа k, и $d_0 = (d_1, d_2)$, то d_1-периодическая функция сохраняет (абсолютно сохраняет) d_2-разности в том и только том случае, когда она сохраняет (абсолютно сохраняет) d_0-разности.*

Лемма 3. *Пусть $d = p_1^{\alpha_1} \dots p_s^{\alpha_s}$, $s \geqslant 2$, $(d, e) = 1$, $k = p_1^{\beta_1} \dots p_s^{\beta_s} e$ и $\beta_i \geqslant \alpha_i$ при $i = 1, \dots, s$. Пусть также $2 \leqslant r \leqslant s$, $d = d_1 \dots d_r$, где $d_1, \dots, d_r$ — попарно взаимно простые числа, $K = C(p_1^{\beta_1}, \dots, p_s^{\beta_s}, e)$, и $f(\widetilde{x})$ — это d-периодическая функция класса K. Тогда функцию f можно представить в виде*

$$f(\widetilde{x}) = f(\widetilde{0}) + \sum_{j=1}^{r} f_j(\widetilde{x}), \tag{2}$$

где $f_j(\widetilde{x})$ — это d_j-периодические функции класса K, определяемые однозначно и удовлетворяющие условию $f_j(\widetilde{x}) \equiv 0 \pmod{k/d_j}$.

Доказательство. Положим $d_i' = p_i^{\alpha_i}$, $i = 1, \dots, s$. Покажем, что функцию $f(\widetilde{x})$ можно представить в виде

$$f(\widetilde{x}) = f(\widetilde{0}) + \sum_{i=1}^{s} f_i'(\widetilde{x}), \tag{3}$$

где $f_i'(\widetilde{x})$ — это d_i'-периодические функции класса K, определяемые однозначно.

Положим $F(\widetilde{x}) = f(\widetilde{x}) - f(\widetilde{0})$. Тогда $F(\widetilde{0}) = 0$. Определим для $i = 1, \dots, s$ значения функций $f_i'(\widetilde{x})$ следующим образом: $f_i'(\widetilde{x}) = F(\widetilde{y}^{(i)})$, где

$$\widetilde{y}^{(i)} \equiv \widetilde{x} \pmod{d_i'}, \tag{4}$$

$$\widetilde{y}^{(i)} \equiv \widetilde{0} \pmod{k/d_i'}. \tag{5}$$

Нетрудно проверить, что если значения i и $\widetilde{x}$ фиксированы, то в E_k^n существует ровно один вектор $\widetilde{y}^{(i)}$, удовлетворяющий условиям (4) и (5), что доказывает d_i'-периодичность функции $f_i'(\widetilde{x})$. Покажем выполнимость равенства (3), которое эквивалентно сравнениям

$$F(\widetilde{x}) \equiv F(\widetilde{y}^{(1)}) + \dots + F(\widetilde{y}^{(s)}) \tag{6}$$

по модулям $e, p_1^{\beta_1}, \dots, p_s^{\beta_s}$.

Во-первых, $F(\widetilde{x})$ — это d-периодическая функция класса $C(e)$, поэтому, согласно следствию 1, все ее значения сравнимы между собой по модулю e, и сравнение (6) по модулю e выполняется.

Далее, фиксируем i, $1 \leqslant i \leqslant s$. Заметим, что из условия (4) следует, согласно лемме 1, что $F(\widetilde{y}^{(i)}) \equiv F(\widetilde{x}) \pmod{p_i^{\beta_i}}$. Если же $1 \leqslant l \leqslant s$ и $l \neq i$, то d_l' является делителем числа k/d_i' и $d_l' = (p_l^{\beta_l}, d)$. Поэтому из условия (5) получаем соотношения

$$F(\widetilde{y}^{(i)}) \equiv F(\widetilde{0}) \equiv 0 \pmod{p_l^{\beta_l}}. \tag{7}$$

Тем самым доказано, что сравнение (6) выполнено и по модулю $p_l^{\beta_l}$ и, следовательно, равенство (3) имеет место.

Покажем, что $f_i'(\widetilde{x}) \in K$ *при* $i = 1, \ldots, s$. *Во-первых,* $f_i'(\widetilde{x}) \equiv 0 \pmod{e}$, так как $F(\widetilde{x}) \equiv 0 \pmod{e}$, и, следовательно, $f_i'(\widetilde{x}) \in C(e)$. Во-вторых, функция $f_i'(\widetilde{x})$ является d_i'-периодической, а значит и $p_i^{\beta_i}$-периодической (так как $d_i' | p_i^{\beta_i}$), поэтому $f_i'(\widetilde{x}) \in C(p_i^{\beta_i})$. Наконец, пусть $1 \leqslant l \leqslant s$, $l \neq i$. Из условий (5) и (7) следует сравнение $f_i'(\widetilde{x}) \equiv 0 \pmod{p_l^{\beta_l}}$, поэтому $f_i'(\widetilde{x}) \in C(p_l^{\beta_l})$.

Для завершения доказательства осталось получить представление (2) из построенных функций $f_i'(\widetilde{x})$. Если $d_j = d_{j_1}' \ldots d_{j_t}'$, то $f_j(\widetilde{x}) = f_{j_1}'(\widetilde{x}) + \ldots + f_{j_t}'(\widetilde{x})$. Лемма доказана.

Лемма 4. *Пусть выполнены условия леммы 3 и, кроме того,* $f(\widetilde{x}) \in C(d_0)$, *где* $d_0 | k$ *и* $d_0 \notin \{p_1^{\beta_1}, \ldots, p_s^{\beta_s}, e\}$. *Тогда* $f_j(\widetilde{x}) \in C(d_0)$, $j = 1, \ldots, r$.

Доказательство. Пусть $e = p_{s+1}^{\beta_{s+1}} \ldots p_t^{\beta_t}$. Достаточно показать, что каждая из функций $f_i'(\widetilde{x})$, определенных при доказательстве леммы 3, принадлежит классу $C(d_0)$ для делителей d_0 числа k, имеющих вид $d_0 = p_l^m$, где $l = 1, \ldots, t$ и $m = 1, \ldots, \beta_l$.

Если $l > s$, то $f_i'(\widetilde{x}) \equiv 0 \pmod{p_l^{\beta_l}}$, следовательно, $f_i'(\widetilde{x}) \in C(p_l^m)$ при $m = 1, \ldots, \beta_l$.

Если $l = i$ и $m \geqslant \alpha_i$, то функция $f_i'(\widetilde{x})$ принадлежит классу $C(p_l^m)$ в силу своей $p_i^{\alpha_i}$-периодичности.

Пусть $l = i$, $m < \alpha_i$ и $\widetilde{x} \equiv \widetilde{x}' \pmod{p_i^m}$. Тогда $f_i'(\widetilde{x}) = F(\widetilde{y})$, $f_i'(\widetilde{x}') = F(\widetilde{y}')$, где $\widetilde{y} \equiv \widetilde{x}$, $\widetilde{y}' \equiv \widetilde{x}' \pmod{p_i^{\alpha_i}}$. При этом $\widetilde{y} \equiv \widetilde{y}' \pmod{p_i^m}$. Функция $F(\widetilde{x})$, так же, как и $f(\widetilde{x})$, сохраняет сравнение по модулю p_i^m, поэтому $f_i'(\widetilde{x}) \in C(p_i^m)$.

Наконец, если $1 \leqslant l \leqslant s$ и $l \neq i$, то $f_i'(\widetilde{x}) \equiv 0 \pmod{p_l^{\beta_l}}$, поэтому $f_i'(\widetilde{x}) \in C(p_l^m)$ при $m = 1, \ldots, \beta_l$. Лемма доказана.

Следствие 2 [6, 9]. *Пусть* $k = k_1 \ldots k_s$, *где* $s \geqslant 2$, *а* $k_1, \ldots, k_s$ — *попарно взаимно простые числа, и* $f(\widetilde{x}) \in C(k_1, \ldots, k_s)$. *Тогда функцию* f *можно представить в виде*

$$f(\widetilde{x}) = f(\widetilde{0}) + \sum_{i=1}^{s} f_i(\widetilde{x}),$$

где $f_i(\widetilde{x})$ — *это* k_i-*периодические функции класса* $C(k_1, \ldots, k_s)$, *определяемые однозначно и удовлетворяющие условию* $f_i(\widetilde{x}) \equiv 0 \pmod{k/k_i}$. *Если при этом* $f(\widetilde{x}) \in M(k)$, *то и* $f_i(\widetilde{x}) \in M(k)$, $i = 1, \ldots, s$.

Лемма 5. *Пусть* d *и* e — *взаимно простые делители числа* k, *и* $h_n(x_1, \ldots, x_n) = eg_d(x_1, \ldots, x_n)$. *Тогда* $h_n(\widetilde{x}) \in [\{1, x+y, h_2(x, y)\}]$ *при всех* $n \geqslant 1$, *а если* $d \neq 2$, *то* $h_n(\widetilde{x}) \in [\{1, x+y, h_1(x)\}]$ *при всех* $n \geqslant 1$.

Доказательство. Нетрудно видеть, что $h_1(x) = h_2(x, x)$ и при $n \geqslant 2$ справедливо равенство $h_{n+1}(\widetilde{x}, y) = h_2(e - h_n(\widetilde{x}), y)$, а если $d \neq 2$, то $h_2(x, y) = h_1(2e - h_1(x) - h_1(y))$.

Замечание 1. Если $k = 2e$ и e нечетно, то $eg_2(x) = e(1 + x) \in L$. В то же время, если $n \geqslant 2$, то $eg_2(x_1, \ldots, x_n) \notin L$ (напомним, что $L = R(1)$), в чем легко убедиться с помощью леммы 3 статьи [11].

Утверждение 1. *Пусть $s \geqslant 2$, и $k_1, \ldots, k_s$ — попарно взаимно простые числа, $k = k_1 \ldots k_s$, $d_i = k/k_i$ при $i = 1, \ldots, s$. Тогда система функций*

$$A = \Big(\bigcup_{i=1}^{s} \{d_i g_{k_i}(x, y)\}\Big) \cup \{1, x+y\}$$

является полной в классе $C(k_1, \ldots, k_s)$, и для всех чисел $k_i \neq 2$ функции $d_i g_{k_i}(x, y)$ в этой системе можно заменить на $d_i g_{k_i}(x)$.

Включение $[A] \subseteq C(k_1, \ldots, k_s)$ нетрудно доказать индукцией по сложности формулы над A, задающей функцию из $[A]$. Обратное включение вытекает из следствия 2 и леммы 5.

Замечание 2. d-периодические функции k-значной логики могут найти применение при описании различных периодических процессов в конечных системах, встречающихся в живой и неживой природе, обществе, технике, а также в математике. Так, функция $g_d(x)$ оказалась подходящим дискретным аналогом «дельта»-функции Дирака при построении обратного преобразования Фурье над конечным полем [17].

§ 2. Классы $R(d) \cap C(e)$ при $(d, e) = 1$, $k = de$

Всюду в данном параграфе $k = de$, $(d, e) = 1$, $1 < d < k$, $1 < e < k$.

Теорема 1. *Имеет место равенство $R(d) \cap C(e) = L(d) \cap M(e)$.*

Доказательство. Соотношение $L(d) \cap M(e) \subseteq R(d) \cap C(e)$ очевидно. Докажем обратное включение.

Пусть $f(\tilde{x}) \in R(d) \cap C(e)$, тогда $f(\tilde{x}) \in C(d, e)$. Согласно следствию 2 функцию f можно представить в виде

$$f(\tilde{x}) = f(\tilde{0}) + f_d(\tilde{x}) + f_e(\tilde{x}), \tag{8}$$

где $f_d(\tilde{x})$ и $f_e(\tilde{x})$ — это d-периодическая и, соответственно, e-периодическая функции класса $C(d, e)$, определяемые однозначно и удовлетворяющие условиям

$$f_d(\tilde{x}) \equiv 0 \pmod{e}, \qquad f_e(\tilde{x}) \equiv 0 \pmod{d}. \tag{9}$$

Тогда $f_e(\tilde{x}) = f(\tilde{x}) - f(\tilde{0}) - f_d(\tilde{x})$. Из последнего равенства следует, что $f_e(\tilde{x}) \in R(d)$. Из соотношений $R(d) \cap R(e) = R(1) = L$ следует, что

$$f(\tilde{0}) + f_e(\tilde{x}) \in L. \tag{10}$$

Кроме того, $f_d(\tilde{x}) \in L(d)$ и из равенства (8) следует, что $f(\tilde{x}) \in L(d)$. Далее, в силу (9), $f_d(\tilde{x}) \in M(e)$, и из представления (8) заключаем, что $f(\tilde{x}) \in M(e)$. Теорема доказана.

Заметим, что из соотношений (8) и (10) вытекает следующий факт.

Лемма 6. *Если $f(\tilde{x}) \in R(d) \cap C(e)$, то функцию f можно представить в виде $f(\tilde{x}) = l(\tilde{x}) + eg(\tilde{x})$, где $l(\tilde{x})$ — это линейная, а $g(\tilde{x})$ — d-периодическая функции, определенные однозначно.*

Следствие 3. *Имеет место равенство $R(p) \cap C(e) = L(p) \cap M(k)$.*

Утверждение 2. *Пусть*

$$A = \{1, x+y, eg_d(x, y)\}, \qquad A_1 = \{1, x+y, eg_d(x)\}.$$

Тогда система функций A является полной в классе $R(d) \cap C(e)$, а система A_1 является полной в этом классе только при $d \neq 2$.

Доказательство. Обозначим для краткости рассматриваемый класс через K. Очевидны соотношения $A \subseteq K$ и $A_1 \subseteq K$, и в силу замкнутости класса K получаем $[A_1] \subseteq [A] \subseteq K$. Включение $K \subseteq [A]$ следует из лемм 6 и 5. Из леммы 5 и замечания 1 следует также, что соотношение $K \subseteq [A_1]$ справедливо только при $d \neq 2$.

Следствие 4. *Если $k = 2e$ и e нечетно, то все одноместные функции класса $R(2) \cap C(e)$ являются линейными.*

Лемма 7. *Пусть $k = pd$, $(p, d) = 1$, $f(\widetilde{x}) \notin C(p)$. Тогда $g_d(x, y) \in [\{1, x+y, pg_d(x, y), f(\widetilde{x})\}]$.*

Доказательство. Если $f(x_1, \ldots, x_n) \notin C(p)$, то при $n \geqslant 2$ подстановкой констант на места переменных функции f из нее можно получить (см. [15, § 17]) одноместную функцию $f_1(x)$, также не принадлежащую классу $C(p)$ (если $n = 1$, то $f_1(x) = f(x)$). При этом найдутся такие α, β из E_k, что $f_1(\alpha) \not\equiv f_1(\beta) \pmod p$. Без ограничения общности полагаем $\beta = f_1(\beta) = 0$, в противном случае применим линейные преобразования функции и переменной. Итак, $f_1(0) = 0$, $f_1(ip) = \gamma$, $(\gamma, p) = 1$ при некотором i, $1 \leqslant i \leqslant d-1$. Построим функцию $h(x)$, удовлетворяющую условиям $h(0) = 0$, $h(ip) = 1$. Если $(\gamma, d) = 1$, то $(\gamma, k) = 1$ и $h(x) = \gamma^{-1} f_1(x)$. Если же $(\gamma, d) > 1$, то рассмотрим функцию $f_2(x) = f_1(x) - pg_d(ip - x)$. Нетрудно проверить, что $f_2(0) = 0$, $f_2(ip) = \gamma - p = \delta$ и $(\delta, k) = 1$. Тогда $h(x) = \delta^{-1} f_2(x)$. Наконец, $g_d(x, y) = h(ipg_d(x, y))$. Лемма доказана.

Теорема 2. *Класс $L(d) \cap M(e)$ является предполным в классе $L(d)$ в том и только том случае, когда $e = p$.*

Доказательство. Если $e = ab$, $a \neq 1$, $b \neq 1$, то имеют место включения

$$L(d) \cap M(ab) \subset L(d) \cap C(a) \subset L(d),$$

так как, например, $ag_d(x, y) \in (L(d) \cap C(a)) \setminus C(ab)$, $g_d(x) \in L(d) \setminus C(a)$, и между $L(d) \cap M(ab)$ и $L(d)$ есть по крайней мере один промежуточный класс.

Пусть $k = pd$, $f \in L(d) \setminus C(p)$. Напомним, что $L(d) = [\{1, x+y, g_d(x, y)\}]$ (см. [11, следствие 5]) и в силу теоремы 1 и утверждения 2 имеем:

$$L(d) \cap M(p) = R(d) \cap C(p) = [\{1, x+y, pg_d(x, y)\}].$$

Применяя лемму 7, убеждаемся в том, что $[(L(d) \cap M(p)) \cup \{f\}] = L(d)$. Теорема доказана.

Следующее утверждение является усиленной формулировкой лемм 22 и 23 статьи [11]. Доказательство, приведенное в [11], не изменяется.

Лемма 8. *Пусть $k \neq 2d$, $n \geqslant 2$, $f(x_1, \ldots, x_n) \in C(d) \setminus R(d)$. Тогда подстановкой на места переменных функции f элементов класса L можно получить одноместную функцию класса $C(d)$, также не сохраняющую d-разности.*

Теорема 3. *Класс L является предполным в классе $L(d) \cap M(e)$ в том и только том случае, когда $d = p$.*

Доказательство. Если $d = ab$, $a \neq 1$, $b \neq 1$, то имеют место включения

$$L \subset L(a) \cap M(e) \subset L(d) \cap M(e),$$

так как, например,

$$eg_a(x, y) \in L(a) \cap M(e) \setminus L, \qquad eg_d(x, y) \in L(d) \cap M(e) \setminus L(a).$$

Пусть $k = pe$, $(p, e) = 1$. Напомним, что $L(p) \cap M(e) = [\{1, x + y, eg_p(x, y)\}]$, и если $p \neq 2$, то полной в этом классе является и система $\{1, x + y, eg_p(x, y)\}$. Пусть $f(\widetilde{x}) \in L(p) \cap M(e) \setminus L$. Функцию f можно, согласно лемме 6, представить в виде $f(\widetilde{x}) = l(\widetilde{x}) + h(\widetilde{x})$, где $l(\widetilde{x}) \in L$, а функция $h(\widetilde{x})$ является p-периодической. Вычитая из функции $f(\widetilde{x})$ линейную функцию $l(\widetilde{x})$, получим p-периодическую функцию $h(\widetilde{x})$, обладающую свойствами: $h(\widetilde{x}) \equiv 0 \pmod e$, $h(\widetilde{x}) \notin L$, $h(\widetilde{0}) = 0$. Далее рассмотрим два случая.

Случай $p=2$. Пусть функция h зависит от n переменных. Тогда $n \geqslant 2$, так как при $n=1$ функция была бы линейной (см. замечание 1). Если $n>2$, то применим лемму 22 статьи [11] и получим подстановкой констант двухместную функцию $H(x, y)$ (если $n=2$, то $H(x, y)=h(x, y)$). Заметим, что $H(0,1)=H(1,0)=0$ (это следует из способа построения функции $l(\widetilde{x})$). Далее, 2-периодическая функция $H(x, y)$ нелинейна, поэтому $H(1,1)=ej$, $1 \leqslant j \leqslant e-1$. Тогда $eg_2(x, y)=j^{-1} H(x+1, y+1)$. Итак, $eg_2(x, y) \in[L \cup\{f\}]$, что доказывает предполноту L в классе $L(2) \cap M(e)$.

Случай $p \neq 2$. Если функция h зависит от n переменных и $n \geqslant 2$, то, применив лемму 8, получим одноместную функцию $H(x)$, в противном случае ($n=1$) положим $H(x)=h(x)$. Далее повторяем рассуждения, изложенные в статье [11] при доказательстве теоремы 9. Заметим только, что $H(1)=0$, поэтому сложность $N(H)$ функции H удовлетворяет неравенствам $1 \leqslant N(H) \leqslant p-2$, и случай 4 невозможен. Итак, класс L предполон в $L(p) \cap M(e)$, и теорема доказана.

§ 3. Замкнутые классы полиномов в $p_1 \ldots p_s$-значной логике

В [5] анализировалась решетка замкнутых классов, находящихся между классом Pol всех функций, представимых полиномами, и классом L. Полностью построена решетка таких классов при $k=4$ (4 — минимальное составное число). В данном разделе мы рассмотрим аналогичную решетку в случае $k=p_1 \ldots p_s$.

Всюду в данном параграфе $k=p_1 \ldots p_s$, $s \geqslant 2$, $d_i=k/p_i$, индексы $i, j, i_1, \ldots, i_t$ принимают значения из множества $\{1, \ldots, s\}$.

Утверждение 3 [1, 11, 14]. *Имеют место равенства*

$$\mathrm{Pol}=M(k)=C(p_1, \ldots, p_s).$$

Следствие 5. *Система функций*

$$\Bigl(\bigcup_i\{d_i g_{p_i}(x, y)\}\Bigr) \cup\{1, x+y\}$$

является полной в классе $M(k)$, и для всех чисел $p_i \neq 2$ функции $d_i g_{p_i}(x, y)$ в этой системе можно заменить на $d_i g_{p_i}(x)$.

Пусть $d \mid k$. Из теоремы 1 следует равенство $M(k) \cap R(d)=M(k) \cap L(d)$. Эти классы будем в дальнейшем обозначать как $ML(d)$.

Утверждение 4. *Пусть $f(\widetilde{x}) \in ML(d_i)$. Тогда функцию f можно представить в виде*

$$f(\widetilde{x})=l(\widetilde{x})+\sum_{j \neq i} h_j(\widetilde{x}), \tag{11}$$

где $l(\widetilde{x}) \in \dot{L}$, а $h_j(\widetilde{x})$ — это p_j-периодические функции, определяемые однозначно и удовлетворяющие условию

$$h_j(\widetilde{x}) \equiv 0 \pmod{d_j}. \tag{12}$$

Доказательство. Имеем $f(\widetilde{x}) \in L(d_i)$, поэтому функцию f можно, согласно лемме 6, представить в виде суммы однозначно определенных линейной функции $l(\widetilde{x})$ и d_i-периодической функции $h(\widetilde{x})$. Далее, функцию h можно, в соответствии с леммой 3, представить в виде

$$h(\widetilde{x})=\sum_{j \neq i} h_j(\widetilde{x}),$$

где $h_j(\widetilde{x})$ — это однозначно определяемые p_j-периодические функции, удовлетворяющие условию (12).

Утверждение 5. *Система функций*

$$A_i = \Big(\bigcup_{j\neq i}\{d_j g_{p_j}(x, y)\}\Big) \cup \{1, x+y\}$$

является полной в классе $ML(d_i)$, *и для всех чисел* $p_j \neq 2$ *функции* $d_j g_{p_j}(x, y)$ *в этой системе можно заменить на* $d_j g_{p_j}(x)$.

Доказательство. Индукцией по сложности формулы над A_i, задающей функцию из $[A_i]$, нетрудно проверить, что $[A_i] \subseteq ML(d_i)$. Докажем обратное включение. Всякая функция f класса $ML(d_i)$ допускает представление (11), а каждую из функций h_j можно представить в виде

$$h_j(\widetilde{x}) = \sum_{\widetilde{\mu}\in E_{p_j}^n} a(\widetilde{\mu}) d_j g_{p_j}(\widetilde{x}-\widetilde{\mu}),$$

где $a(\widetilde{\mu}) \in E_{p_j}$. Согласно лемме 5 при любом $n \geqslant 1$ имеем $d_j g_{p_j}(x_1, \ldots, x_n) \in \in [A_i]$, а если $p_j \neq 2$, то $d_j g_{p_j}(x_1, \ldots, x_n) \in [\{1, x+y, d_j g_{p_j}(x)\}]$. Утверждение доказано.

Пусть $I \subseteq \{1, \ldots, s\}$. Введем замкнутые классы

$$ML(I) = \bigcap_{i\in I} ML(d_i).$$

Следствие 6. *Справедливы следующие соотношения.*

1. *Если* $I=\{i_1, \ldots, i_t\}$, *то* $ML(I) = ML(d)$, *где* $d=(d_{i_1}, \ldots, d_{i_t}) = \prod_{j\notin I} p_j$.
2. $ML(\{1, \ldots, s\}) = ML(1) = L$.
3. $ML(\varnothing) = M(k) = \mathrm{Pol}$.
4. *Если* $I_1 \subseteq I_2$, *то* $ML(I_2) \subseteq ML(I_1)$.

Эти факты вытекают из теорем 4 и 5 статьи [11] и утверждения 3.

Аналогично утверждениям 4 и 5 доказываются следующие результаты.

Утверждение 6. *Если* $f(\widetilde{x}) \in ML(I)$, *то функцию* f *можно представить в виде*

$$f(\widetilde{x}) = l(\widetilde{x}) + \sum_{j\notin I} h_j(\widetilde{x}), \tag{13}$$

где $l(\widetilde{x}) \in L$, *а* $h_j(\widetilde{x})$ — *это* p_j*-периодические функции, определяемые однозначно и удовлетворяющие условию* (12).

Утверждение 7. *Система функций*

$$\Big(\bigcup_{j\notin I}\{d_j g_{p_j}(x, y)\}\Big) \cup \{1, x+y\}$$

является полной в классе $ML(I)$, *и для всех чисел* $p_j \neq 2$ *функции* $d_j g_{p_j}(x, y)$ *в этой системе можно заменить на* $d_j g_{p_j}(x)$.

Теорема 4. *Пусть* $I' = I \cup \{i'\}$. *Тогда класс* $ML(I')$ *является предполным в классе* $ML(I)$.

Доказательство. Пусть $f(x_1, \ldots, x_n) \in ML(I') \setminus ML(\{i'\})$. Учитывая утверждение 7, достаточно показать, что $d_{i'} g_{p_{i'}}(x, y) \in [ML(I') \cup \{f\}]$. Функцию f, согласно утверждению 6, можно представить в виде (13). При этом линейная функция $l(\widetilde{x})$ и p_j-периодические функции $h_j(\widetilde{x})$ принадлежат классу $ML(I')$ (так как $p_j | d_{i'}$). Следовательно, вычитая из функции f функции класса $ML(I')$, получим $p_{i'}$-периодическую функцию $h_{i'}(x_1, \ldots, x_n)$, все значения которой кратны $d_{i'}$. Из условия $f \notin ML(I')$

следует, что $h_{i'}(\tilde{x}) \notin ML(I')$. Далее, $h_{i'}(x_1, \ldots, x_n) \in C(d_{i'}) \setminus R(d_{i'})$ согласно теореме 1. Если $n > 2$, то применяя лемму 22 статьи [11], из функции $h_{i'}$ подстановкой констант получим функцию H, зависящую не более чем от двух переменных и удовлетворяющую условию $H \in C(d_{i'}) \setminus R(d_{i'})$. Очевидно, функция H нелинейна, т. е. $H \notin R(1)$. Далее из функции H построим функцию $d_{i'} g_{p_{i'}}(x)$, если $p_{i'} \neq 2$, или $d_{i'} g_2(x, y)$ таким же образом, как при доказательстве теоремы 9 в статье [11] построены функции $\psi_d(x)$ и $\psi_d(x, y)$ в случаях $k \neq 2d$ и $k = 2d$ соответственно. Разница имеется только в следующих деталях доказательства.

1. Условие $H \notin R(d)$ заменяется условием $H \notin R(1)$.
2. Вместо d-периодических функций используем линейные, вместо $\chi_d(x)$ — функцию $d_{i'} x$.
3. В качестве S берем множество $\{0, 1\}$.
4. Значения функции кратны не d, а $d_{i'}$.
5. Вместо леммы 23 применяем лемму 8 настоящей статьи.
6. d-решеточное ограничение функции не выделяется.

Итак, если $p_{i'} = 2$, то нами построена требуемая функция $d_{i'} g_2(x, y)$. Если $p_{i'} \neq 2$, то нами построена функция $d_{i'} g_{p_{i'}}(x)$, и доказательство завершается применением леммы 5.

Следствие 7. *Между классами $M(k)$ и L находится ровно $2^s - 2$ замкнутых класса. Каждый из них имеет вид $ML(I)$, $I \subset \{1, \ldots, s\}$. Эти классы (вместе с $M(k)$ и L) образуют решетку, изоморфную s-мерному единичному кубу. Атомами решетки являются классы $ML(p_i)$, коатомами — классы $ML(d_i)$, $i = 1 \ldots, s$.*

Следствие 8. *Система полиномов, содержащая все линейные функции, полна в классе* Pol *тогда и только тогда, когда она содержит функции, не сохраняющие d_i-разности для $i = 1, \ldots, s$.*

Замечание 3. В классе Pol имеются универсальные (шефферовы) функции. Примером может служить предложенная В. Ш. Дарсалия функция $xy - yz + y + 1$, являющаяся также универсальной в более обширном классе всех полиномов с целыми коэффициентами [4].

§ 4. О сложности задания функций

Определение. Минимальное количество числовых значений, достаточное для однозначного определения n-местной функции $f(x_1, \ldots, x_n)$, будем называть *сложностью задания функции* f и обозначать как $I_n(f)$.

Сложность задания функции характеризует объем памяти, достаточный для хранения всей информации о функции.

Следствие 9. *Имеют место следующие оценки сложности задания функций.*

1. *Для любой функции f из P_k справедливо неравенство $I_n(f) \leqslant k^n$.*
2. *Если функция f является d-периодической, то $I_n(f) \leqslant d^n$.*
3. *Если $f \in L$, то $I_n(f) \leqslant n + 1$.*
4. *Если $f \in R(d)$, то $I_n(f) \leqslant d^n(n+1)$.*
5. *Если $f \in L(d)$, то $I_n(f) \leqslant d^n + n$.*
6. *Если $k = k_1 \ldots k_s$, где $s \geqslant 2$, числа $k_1, \ldots, k_s$ попарно взаимно простые, $f \in C(k_1, \ldots, k_s)$, то $I_n(f) \leqslant k_1^n + \ldots + k_s^n + 1$.*
7. *Если $k = p_1 \ldots p_s$, $s \geqslant 2$, $I \subseteq \{1, \ldots, s\}$, $f \in ML(I)$, то*

$$I_n(f) \leqslant n + 1 + \sum_{j \in \{1, \ldots s\} \setminus I} p_j^n.$$

§ 5. Классы $L(d)$ и $R(d)$

Пусть d — собственный делитель числа k. В данном параграфе мы найдем условия, при которых класс $L(d)$ является предполным в классе $R(d)$.

Как было отмечено выше, система функций $\{1, x+y, g_d(x,y)\}$ полна в классе $L(d)$. Введем функции

$$\chi_d(\widetilde{x}) = x_n g_d(\widetilde{x}), \qquad \delta_d(x) = d\lfloor x/d \rfloor$$

(через $\lfloor r \rfloor$ обозначаем целую часть рационального числа r). Установлено (см. [11, § 3]), что $\chi_d(\widetilde{x}) \in R(d) \setminus L(d)$, $\delta_d(x) \in L(d)$, и система функций $\{1, x+y, g_d(x,y), \chi_d(x,y)\}$ полна в классе $R(d)$, причем при $d \neq 2$ функцию $g_d(x,y)$ в этой системе можно заменить на $g_d(x)$. Мы покажем, что и функцию $\chi_d(x,y)$ можно заменить одноместной функцией $\chi_d(x)$ при любом d. Обозначим количество переменных функции верхним индексом в скобках у функционального символа. Нетрудно проверить справедливость следующего факта.

Лемма 9. *Имеет место соотношение*

$$\chi_d^{(2)}(x,y) = \chi_d^{(1)}(x + \chi_d^{(1)}(y)) - \chi_d^{(1)}(x).$$

Следствие 10. *Система функций $\{1, x+y, g_d(x,y), \chi_d(x)\}$ является полной в классе $R(d)$, а если $d \neq 2$, то функцию $g_d(x,y)$ можно заменить на $g_d(x)$.*

Лемма 10. *Пусть $n \geqslant 1$ и $(n+1)$-местная функция сохраняет d-разности, но не абсолютно. Тогда с помощью элементов класса $L(d)$ из нее можно получить одноместную функцию $h(x)$ такую, что $h(x) \in$ $\in R(d) \setminus L(d)$.*

Доказательство. Рассмотрим $(n+1)$-местную функцию $f(\widetilde{x}, y)$ такую, что $f \in R(d) \setminus L(d)$. Без ограничения общности можно считать, что не абсолютно сохраняются d-разности по последней, $(n+1)$-й переменной y, т. е. величины $\Delta_{n+1} f(\widetilde{x}, y)$ зависят от $\widetilde{x}$ и y. Рассмотрим эти разности как функцию переменных $\widetilde{x}$ и y.

Если $\Delta_{n+1} f(\widetilde{x}, y)$ существенно зависит от y, то требуемая функция $h(y)$ получается из $f(\widetilde{x}, y)$ подстановкой констант вместо переменных $\widetilde{x}$.

Пусть $\Delta_{n+1} f(\widetilde{x}, y)$ не зависит существенно от переменной y, а зависит только от $\widetilde{x}$, точнее, от наименьших неотрицательных вычетов $\widetilde{\mu}$ компонент вектора $\widetilde{x}$ по модулю d. Можно считать что $\Delta_{n+1} f(\widetilde{0}, y) = 0$ (в противном случае, если $\Delta_{n+1} f(\widetilde{0}, y) = Ad \neq 0$, этого добьемся, рассматривая вместо $f(\widetilde{x}, y)$ функцию $f(\widetilde{x}, y) - Ay$). Пусть при некотором $\widetilde{\mu}$, $\widetilde{\mu} \in E_d^n \setminus \{\widetilde{0}\}$, имеем $\Delta_{n+1} f(\widetilde{\mu}, y) = Bd \neq 0$. Положим $h(x) = f(\mu_1 g_d(x), \ldots, \mu_n g_d(x), x)$. Заметим, что $h(x) \in R(d)$ в силу замкнутости класса $R(d)$. Далее,

$$\Delta h(0) = h(d) - h(0) = f(\widetilde{\mu}, d) - f(\widetilde{\mu}, 0) = \Delta_{n+1} f(\widetilde{\mu}, 0) = Bd,$$

$$\Delta h(1) = h(1+d) - h(1) = f(\widetilde{0}, d+1) - f(\widetilde{0}, 1) = \Delta_{n+1} f(\widetilde{0}, 1) = 0$$

в силу того, что функция $\Delta_{n+1} f(\widetilde{x}, y)$ не зависит существенно от переменной y. Таким образом, $h(x) \in R(d) \setminus L(d)$. Лемма доказана.

Теорема 5. *Класс $L(d)$ является предполным в классе $R(d)$ в том и только том случае, когда $k = pd$.*

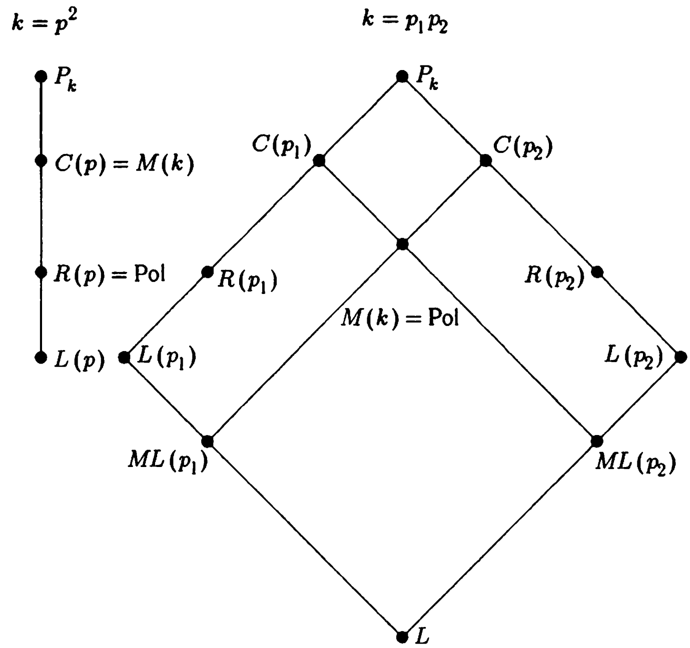
Доказательство. Пусть $k = abd$. Тогда имеют место включения $L(d) \subset L(ad) \cap R(d) \subset R(d)$, так как, например,

$$b\chi_d(x) \in L(ad) \cap R(d) \setminus L(d), \qquad \chi_d(x) \in R(d) \setminus L(ad).$$

Пусть теперь $k = pd$ и $f \in R(d) \setminus L(d)$. Можем считать функцию f одноместной, в противном случае применим лемму 10. Вычитая d-периодическую функцию из функции $f(x)$, получим функцию $h(x)$, такую, что $h(x) = 0$ на множестве E_d и $h(x) \equiv 0 \pmod d$. Пусть $h(d) = Ad$. Положим $h_1(x) = h(x) - A\delta_d(x)$. Тогда $h_1(x) = 0$, если $x \equiv 0 \pmod d$. Так как $f(x), h(x), h_1(x) \notin L(d)$, то при некотором i, $1 \leqslant i \leqslant d-1$, имеем $h_1(d+i) = Bd \neq 0$. Заметим также, что $h_1(x) \in R(d)$, поэтому $h_1(ld+i) = lBd$ при $l = 0, 1, \ldots, p-1$. Далее, положим $h_2(x) = h_1(\delta_d(x) + ig_d(x))$. Нетрудно проверить, что $h_2(x) = B\chi_d(x)$. Очевидно, $(B, p) = 1$. Пусть $C \equiv B^{-1} \pmod p$. Тогда $\chi_d(x) = Ch_2(x) \in [L(d) \cup \{f\}]$ и $[L(d) \cup \{f\}] = R(d)$. Теорема доказана.

Замечание 4. Условие $k = pd$ является также необходимым и достаточным для того, чтобы класс $R(d)$ был предполным в $C(d)$ (см. [11, теорема 9]). Классы $C(d)$ являются предполными в P_k при любых k и $d \neq 1$, $d \neq k$ (см. [15]).

Полученные результаты позволяют построить следующие фрагменты решетки замкнутых классов в P_k при $k = p^2$ и $k = p_1 p_2$.



Замечание 5. В статье [5] для случая $k = 4$ указана полная система $\{1, x+y, x^2y^2\}$ в классе, совпадающем в наших обозначениях с $L(2)$. Нетрудно проверить, что

$$x^2y^2 = g_2(x+1, y+1).$$

СПИСОК ЛИТЕРАТУРЫ

1. Айзенберг Н. Н., Семйон И. В. Некоторые критерии представимости функций k-значной логики полиномами по модулю k // Многоустойчивые элементы и их применение. — М.: Сов. радио, 1971. — С. 84—88.
2. Гаврилов Г. П. О надструктуре класса полиномов в многозначных логиках // Дискретная математика. — 1996. — Т. 8, вып. 3. — С. 90–97.
3. Гаврилов Г. П. О замкнутых классах многозначной логики, содержащих класс полиномов // Дискретная математика. — 1997. — Т. 9, вып. 2. — С. 12–23.

4. Дарсалия В. Ш. Условия полноты для полиномов с натуральными, целыми и рациональными коэффициентами // Фунд. и прикл. матем. — 1996. — Т. 2, Вып. 2. — С. 365–374.
5. Крохин А. А., Сафин К. Л., Суханов Е. В. О строении решетки замкнутых классов полиномов // Дискретная математика. — 1997. — Т. 9, вып. 2. — С. 24–39.
6. Мещанинов Д. Г. Некоторые условия представимости функций из P_k полиномами по модулю // Докл. АН СССР. — 1988. — Т. 299, № 1. — С. 50–53.
7. Мещанинов Д. Г. О некоторых свойствах надструктуры класса полиномов в P_k // Матем. заметки. — 1988. — Т. 44, № 5. — С. 673–681.
8. Мещанинов Д. Г. О вторых p-разностях функций p^α-значной логики // Дискретная математика. — 1992. — Т. 4, вып. 4. — С. 131–139.
9. Мещанинов Д. Г. Метод построения полиномов для функций k-значной логики // Дискретная математика. — 1995. — Т. 7, вып. 3. — С. 48–60.
10. Мещанинов Д. Г. О классе Кузнецова в p^α-значной логике // Тез. докл. XI Междунар. конф., Ульяновск, 10–14 июня 1996 г. — М.: Изд-во РГГУ, 1996. — С. 142–143.
11. Мещанинов Д. Г. О первых d-разностях функций k-значной логики // Математические вопросы кибернетики. Вып. 7. — М.: Наука, 1998. — С. 265–280.
12. Ремизов А. Б. О надструктуре замкнутого класса полиномов по модулю k // Дискретная математика. — 1989. — Т. 1, вып. 1. — С. 3–15.
13. Черепов А. Н. Описание структуры замкнутых классов в P_k, содержащих класс полиномов // Проблемы кибернетики. Вып. 40. — М.: Наука, 1983. — С. 5–18.
14. Черепов А. Н. Надструктура класса сохранения отношений сравнения в k-значной логике по всем модулям-делителям k: Автореф. дис. канд. физ.-мат. наук. — М., 1986.
15. Яблонский С. В. Функциональные построения в k-значной логике // Тр. МИАН СССР. — 1958. — Т. 51. — С. 5–142.
16. Янов Ю. И., Мучник А. А. О существовании k-значных замкнутых классов, не имеющих конечного базиса // Докл. АН СССР. — 1959. — Т. 127, № 1. — С. 44–46.
17. Reed I. S., Truong T. K. The use of finite fields to compute convolations // IEEE Trans. on Inform. Theory. — 1975. — V. IT-21, № 3. — P. 208–213. [Русский перевод: Рид И. С., Трунг Т. К. Применение конечных полей для вычисления сверток // В кн.: Макклеллан Дж. Х., Рейдер Ч. М. Применение теории чисел в цифровой обработке сигналов. — М.: Радио и связь, 1983. — С. 207–216.]

Поступило в редакцию 29 VI 1998