Math-Net.Ru

Общероссийский математический портал

Г. П. Гаврилов, О замкнутых классах многозначной логики, содержащих класс полиномов, *Дискрет. матем.*, 1997, том 9, выпуск 2, 12–23

DOI: <https://doi.org/10.4213/dm465>

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: 54.89.56.158

26 апреля 2023 г., 17:21:20

О замкнутых классах многозначной логики, содержащих класс полиномов

© 1997 г. Г. П. Гаврилов

Для многозначной логики P_k , где $k = p^r$, p — простое число и $r \geq 2$, описываются некоторые семейства замкнутых классов, включающих класс полиномов Pol_k и содержащихся в классе $\mathfrak{M}_k$, состоящем из функций, сохраняющих сравнение по каждому модулю $d = p^j$, $j = 1, \dots, r-1$. Данные замкнутые классы тесно связаны с подмножествами из специальной полной системы класса $\mathfrak{M}_k$. Выявлено существенное различие между случаями, соответствующими $p = 2$ и $p = 3$.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 94-01-01206.

1. Введение

1.1. Основные определения

Положим

$$P_k = \bigcup_{n \geq 0} P_k^{(n)},$$

где $P_k^{(n)}$ — множество всех n -местных функций вида $E_k^n \rightarrow E_k = \{0, 1, \dots, k-1\}$ (здесь $k \geq 3$ и $n \geq 0$). Функции из P_k называются k -значными (а также функциями k -значной, или многозначной, логики). Замыкание на множестве подмножеств из P_k рассматривается относительно операции суперпозиции. Через Pol_k обозначим класс всех полиномиальных функций из P_k , т.е. множество всех функций, представимых полиномами по модулю k . Эти функции мы будем иногда тоже называть полиномами.

Если d — делитель числа k , то через $\mathcal{L}_k(d)$ обозначается множество всех функций из P_k , сохраняющих сравнение по модулю d , т.е. $f(\tilde{x}^n) \in \mathcal{L}_k(d)$ тогда и только тогда, когда для любых двух наборов значений переменных $\tilde{\alpha}^n = (\alpha_1, \dots, \alpha_n)$ и $\tilde{\beta}^n = (\beta_1, \dots, \beta_n)$ таких, что $\alpha_i \equiv \beta_i \pmod{d}$, $i = 1, \dots, n$, справедливо сравнение $f(\tilde{\alpha}^n) \equiv f(\tilde{\beta}^n) \pmod{d}$.

Положим

$$\mathfrak{M}_k = \bigcap_{d|k} \mathcal{L}_k(d).$$

Множества $\mathcal{L}_k(d)$ и $\mathfrak{M}_k$ являются замкнутыми классами в P_k .

В дальнейшем будем считать (если иное не будет оговорено особо), что $k = p^r$, где p — простое число и r — натуральное число, не меньшее 2.

Нам понадобятся следующие специальные функции из класса $\mathfrak{M}_{p^r}$: сумма и произведение по модулю p^r и функции

$$h_l^{(n)}(\tilde{x}^n) = \begin{cases} p^l, & \text{если } \tilde{x}^n \equiv \tilde{0}^n \pmod{p^{l+1}}, \\ 0 & \text{в остальных случаях,} \end{cases}$$

$l = 0, 1, \dots, r-1, n \geq 1$.

Любую функцию $f(\tilde{x}^n) \in P_k$ при $k = p^r$ можно представить в виде

$$f(\tilde{x}^n) = \sum_{i=0}^{r-1} p^i (\theta_i f)(\tilde{x}^n),$$

где функция

$$(\theta_i f)(\tilde{x}^n) = [f(\tilde{x}^n)/p^i] - p[f(\tilde{x}^n)/p^{i+1}]$$

осуществляет отображение вида $E_k^n \rightarrow E_p$, $i = 0, 1, \dots, r-1$. Здесь деление рассматривается в поле $\mathbf{Q}$ и $[b]$ означает целую часть числа $b \in \mathbf{Q}$.

Функцию $(\theta_i f)(\tilde{x}^n)$ будем называть i -й составляющей функции $f(\tilde{x}^n)$.

В работе [1] было доказано, что если $f(\tilde{x}^n) \in \mathfrak{M}_{p^r}$ ($r \geq 2$ и $n \geq 1$), то

$$f(\tilde{x}^n) = \sum_{i=0}^{r-1} \sum_{\tilde{\tau} \in E_{p^{i+1}}^n} ((\theta_i f)(\tilde{\tau})) h_i^{(n)}(\tilde{x}^n - \tilde{\tau}).$$

Исходя из этого формульного представления функций класса $\mathfrak{M}_{p^r}$, мы установили, что

(1) система

$$A_{p^r} = \{1, x + y, xy\} \cup \bigcup_{i=0}^{r-1} \{h_i^{(2)}(\tilde{x}^2)\}$$

(и даже система $A_{p^r} \setminus \{xy\}$) полна в $\mathfrak{M}_{p^r}$, и

(2) при $p \geq 3$ в $\mathfrak{M}_{p^r}$ полна система

$$B_{p^r} = \{1, x + y, xy\} \cup \bigcup_{i=0}^{r-1} \{h_i^{(1)}(x)\}$$

(и даже система $B_{p^r} \setminus \{xy\}$).

Принимая во внимание полиномиальность функций $h_0^{(n)}(\tilde{x}^n)$, мы сформулировали и такое утверждение: в $\mathfrak{M}_{p^r}$ при всяком простом $p \geq 2$ полна система

$$A'_{p^r} = \{1, x + y, xy\} \cup \bigcup_{i=1}^{r-1} \{h_i^{(2)}(\tilde{x}^2)\},$$

а при $p \geq 3$ полна система

$$B'_{p^r} = \{1, x + y, xy\} \cup \bigcup_{i=i}^{r-1} \{h_i^{(1)}(x)\}.$$

1.2. О чем эта работа

Мы рассматриваем здесь замкнутые классы, порождаемые некоторыми подмножествами из систем A'_{p^r} и B'_{p^r} и содержащие класс полиномов Pol_{p^r} . Для установления взаимосвязей между этими классами мы описываем ряд свойств. Класс функций, сохраняющих фиксированное свойство, целиком содержит вполне определенную совокупность из введенных нами замкнутых классов. Тем самым мы получаем некоторую подрешетку замкнутых классов, лежащих между классами Pol_{p^r} и $\mathcal{M}_{p^r}$, и можем высказать несколько утверждений о ширине и других характеристиках решетки $(\text{Pol}_{p^r}; \mathcal{M}_{p^r})$, а также сформулировать ряд необходимых условий полиномиальности функций из класса $\mathcal{M}_{p^r}$.

1.3. Немного истории

То, что любую одноместную функцию из P_k при k , равном простому числу, можно представить полиномом по модулю k , отмечалось еще Шарлем Эрмитом [2] в связи с исследованием так называемых перестановочных многочленов над полями Галуа $\text{GF}(p^r)$. Спустя более чем полвека, Кемпнер [3] доказал, что любая одноместная функция из P_k может быть реализована полиномом по модулю k тогда и только тогда, когда k является простым числом.

Вопросам представимости функций из P_k полиномами по модулю k посвящены работы [4–13]. Интересные результаты в этом направлении получены в последнее время в [14, 15].

Задача о расположении класса Pol_k в структуре (решетке) включений замкнутых классов системы P_k была поставлена впервые С. В. Яблонским в [16]. В этой работе было доказано, что класс Pol_k образует полную (относительно операции суперпозиции) систему в P_k тогда и только тогда, когда k — простое число, и было установлено, кроме того, что при составном k класс Pol_k не является даже предполным (результат А. В. Кузнецова).

В 1972 году автор предложил своему ученику А. Н. Черепову заняться исследованием надструктуры класса Pol_k при составном k . Опираясь на работу [11], довольно быстро удалось выяснить, что в этой надструктуре полезно сначала изучить подструктуру, расположенную над классом $\mathcal{M}_k$, и что классы Pol_k и $\mathcal{M}_k$ совпадают тогда и только тогда, когда k свободно от квадратов. Кроме того, стало ясно, что ряд свойств надструктуры класса Pol_k при $k = p_1^{r_1} \dots p_v^{r_v}$, где $p_1, \dots, p_v$ — различные простые числа, $r_1, \dots, r_v$ — натуральные числа и $v \geq 2$, тесно связаны со свойствами надструктур классов полиномов в системах P_{k_i} , где $k_i = p_i^{r_i}$, $i = 1, \dots, v$. Ряд результатов, полученных в данном направлении, можно найти в работах А. Н. Черепова [17, 18], Д. Г. Мещанинова [19–22] и А. Б. Ремизова [23]. В [17] описана надструктура класса $\mathcal{M}_k$ при k , свободном от квадратов (это как раз тот случай, когда $\mathcal{M}_k = \text{Pol}_k$). В [18] установлено, что надструктура класса $\mathcal{M}_{p^r}$ при $r \geq 2$ изоморфна решетке всех подмножеств множества $\{1, \dots, r-1\}$. В [21] доказано, что при $k = p_1^2 p_2 \dots p_v$, где $p_1, p_2, \dots, p_v$ — различные простые числа, класс Pol_k предполон в $\mathcal{M}_k$. В [19] сформулировано следующее утверждение: при $k = p_1^2 \dots p_t^2 p_{t+1} \dots p_v$, где $p_1, \dots, p_v$ — различные простые числа, класс Pol_k является предполным в $\mathcal{M}_k$, если $t = 1$, а в том случае, когда $t \geq 2$, между классами Pol_k и $\mathcal{M}_k$ имеется $2^t - 2$ замкнутых классов, образующих вместе с Pol_k и $\mathcal{M}_k$ решетку, изоморфную решетке всех подмножеств t -множества. Доказательство приведенного утверждения можно найти в работе [23]. В этой же работе для $k = p^3 q$, где $p \geq 2$

и $q \geq 1$, построена счетная цепочка замкнутых классов, лежащих между классами Pol_k и $\mathfrak{M}_k$, и описан замкнутый класс, не имеющий базиса и содержащий класс Pol_k .

2. Свойство H_i

Пусть i — фиксированное целое число, $1 \leq i \leq r-1$, и $r \geq 2$. Будем говорить, что функция $f(\tilde{x}^n) \in \mathfrak{M}_{p^r}$ обладает свойством $H_i(p^r)$, если функция $(\theta_i f)(\tilde{\tau}^n + p^i \tilde{y}^n)$ при всяком наборе $\tilde{\tau}^n \in E_p^n$ является линейной функцией из P_p (т. е. относительно $\tilde{y}^n \in E_p^n$). Множество всех функций, обладающих свойством $H_i(p^r)$, обозначим через $W_i(p^r)$.

Замечание. Нетрудно показать, что при добавлении и изъятии фиктивных переменных свойство функции, состоящее в принадлежности их множеству $W_i(p^r)$, не нарушается.

Лемма 1. Пусть $p \geq 3$ и $r \geq 2$. Тогда функции $1, h_l^{(1)}(x)$, где $l \neq i$, $x, x_1 + x_2$ и $x_1 x_2$ принадлежат $W_i(p^r)$, а $h_i^{(1)}(x) \notin W_i(p^r)$.

Доказательство. Если $f(x) = 1$ или $f(x) = h_l^{(1)}(x)$, где $l \neq i$, то $(\theta_i f)(\tau + p^i y) \equiv 0$. Очевидно также, что при $f(x) = x$ справедливо равенство $(\theta_i f)(\tau + p^i y) = y$. Рассмотрим функцию $\varphi(x_1, x_2) = x_1 + x_2$. Легко видеть, что

$$(\theta_i \varphi)(\tilde{\tau}^2 + p^i \tilde{y}^2) = \theta_i(\tau_1 + \tau_2 + p^i(y_1 + y_2)) = \theta_i(\tau_1 + \tau_2) \oplus y_1 \oplus y_2,$$

где $\oplus$ — знак сложения по модулю p . Далее, пусть $\psi(x_1, x_2) = x_1 x_2$. Тогда

$$(\theta_i \psi)(\tilde{\tau}^2 + p^i \tilde{y}^2) = \theta_i((\tau_1 + p^i y_1)(\tau_2 + p^i y_2)) = \theta_i(\tau_1 \tau_2) \oplus ((\theta_0(\tau_1)) \circ y_2) \oplus ((\theta_0(\tau_2)) \circ y_1),$$

где $\circ$ — умножение по модулю p . Итак, действительно, каждая из функций $1, h_l^{(1)}(x)$, где $l \neq i$, $x, x_1 + x_2$ и $x_1 x_2$ принадлежит $W_i(p^r)$.

Рассмотрим теперь функцию $f(x) = h_i^{(1)}(x)$. Очевидно, что при $\tau = 0$

$$(\theta_i f)(p^i y) = \begin{cases} 1, & \text{если } y = 0, \\ 0, & \text{если } y = 1, \dots, p-1. \end{cases}$$

Эта функция линейной не является. В самом деле, предположим, что $\varphi_0(y) = (\theta_i f)(p^i y) = a \circ y \oplus b$. Тогда $\varphi_0(0) = b = 1$, $\varphi_0(1) = a \oplus 1 = 0$ и $\varphi_0(2) = 2 \circ a \oplus 1 = 0$, что при $p \geq 3$ невозможно. Лемма доказана.

Лемма 2. Пусть $p = 2$ и $r \geq 2$. Тогда функции $1, x, x_1 + x_2, x_1 x_2, h_l^{(2)}(\tilde{x}^2)$, где $l \neq i$, и $h_i^{(1)}(x)$ принадлежат $W_i(2^r)$, а $h_i^{(2)}(\tilde{x}^2) \notin W_i(2^r)$.

Доказательство. Обоснование того, что функции $x_1 + x_2$ и x_1x_2 принадлежат $W_i(2^r)$, аналогично проведенному в лемме 1. Далее, $(\theta_i h_i^{(2)})(\tilde{\tau}^2 + 2^i \tilde{y}^2) \equiv 0$ при $l \neq i$. Значит, $h_i^{(2)}(\tilde{x}^2) \in W_i(2^r)$ при всяком $l \neq i$. Так как i -я составляющая любой одноместной функции $f(\tau + 2^i y)$ является булевой функцией от y , она, очевидно, линейна. Отсюда следует, что функции 1, x и $h_i^{(1)}(x)$ тоже принадлежат $W_i(2^r)$.

Рассмотрим, наконец, функцию $h_i^{(2)}(\tilde{x}^2)$. Если $\tilde{\tau}^2 = (0, 0)$, то

$$(\theta_i h_i^{(2)})(2^i y_1, 2^i y_2) = \begin{cases} 1, & \text{если } y_1 = y_2 = 0, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Очевидно, что эта функция линейной (в P_2) не является. Лемма доказана.

Лемма 3. Пусть функции $f_0(\tilde{x}^m), f_1(\tilde{x}^n), \dots, f_m(\tilde{x}^n)$, $m \geq 1$, $n \geq 1$, обладают свойством $H_i(p^r)$, где $p \geq 2$ и $r \geq 2$. Тогда функция

$$\Phi(\tilde{x}^n) = f_0(f_1(\tilde{x}^n), \dots, f_m(\tilde{x}^n))$$

тоже обладает свойством $H_i(p^r)$.

Доказательство. Введем обозначения

$$\begin{aligned} (\xi_i f)(\tilde{x}^n) &= \sum_{l=0}^{i-1} p^l ((\theta_l f)(\tilde{x}^n)), \\ (\zeta_i f)(\tilde{x}^n) &= \sum_{l=i+1}^{r-1} p^{l-i-1} ((\theta_l f)(\tilde{x}^n)). \end{aligned}$$

Очевидно, что

$$\begin{aligned} (\xi_i f)(\tilde{x}^n) &: E_{p^r}^n \rightarrow E_{p^i}, \\ (\zeta_i f)(\tilde{x}^n) &: E_{p^r}^n \rightarrow E_{p^{r-i-1}} \end{aligned}$$

(если $i = r + 1$, то полагаем $(\zeta_i f)(\tilde{x}^n) \equiv 0$) и что

$$f(\tilde{x}^n) = (\xi_i f)(\tilde{x}^n) + p^i (\theta_i f)(\tilde{x}^n) + p^{i+1} (\zeta_i f)(\tilde{x}^n). \quad (1)$$

Если $f(\tilde{x}^n) \in \mathfrak{M}_{p^r}$, то при $\tilde{\alpha}^n \equiv \tilde{\beta}^n \pmod{p^i}$

$$f(\tilde{\alpha}^n) \equiv f(\tilde{\beta}^n) \pmod{p^i},$$

а значит, $(\theta_l f)(\tilde{\alpha}^n) = (\theta_l f)(\tilde{\beta}^n)$ для всякого $l < i$. Учитывая этот факт, получаем, что

$$(\xi_i f_s)(\tilde{\tau}^n + p^i \tilde{y}^n) = (\xi_i f_s)(\tilde{\tau}^n), \quad s = 1, \dots, m.$$

Далее, так как для любого l , $0 \leq l \leq r - 1$, справедливо соотношение

$$(\theta_l \Phi)(\tilde{x}^n) = (\theta_l f_0)(f_1(\tilde{x}^n), \dots, f_m(\tilde{x}^n)),$$

принимая во внимание (1), находим, что

$$(\theta_i \Phi)(\tilde{\tau}^n + p^i \tilde{y}^n) = (\theta_i f_0)((\xi_i f_1)(\tilde{\tau}^n) + p^i(\theta_i f_1)(\tilde{\tau}^n + p^i \tilde{y}^n), \dots, (\xi_i f_m)(\tilde{\tau}^n) + p^i(\theta_i f_m)(\tilde{\tau}^n + p^i \tilde{y}^n)). \quad (2)$$

Поскольку функции $f_0, f_1, \dots, f_m$ обладают свойством $H_i(p^r)$,

$$\begin{aligned} (\theta_i f_0)(\tilde{\sigma}^m + p^i \tilde{y}^m) &= a_0(\tilde{\sigma}^m) \oplus \sum_{t=1}^m a_t(\tilde{\sigma}^m) \circ y_t, \\ (\theta_i f_s)(\tilde{\tau}^n + p^i \tilde{y}^n) &= b_{s0}(\tilde{\tau}^n) \oplus \sum_{v=1}^n b_{sv}(\tilde{\tau}^n) \circ y_v, \end{aligned}$$

где $s = 1, \dots, m$, $\oplus$ и $\circ$ — соответственно знаки сложения и умножения по модулю p , и — сумма по модулю p .

Следовательно, в силу (2)

$$\begin{aligned} (\theta_i \Phi)(\tilde{\tau}^n + p^i \tilde{y}^n) &= a_0(\tilde{\sigma}^m) \oplus \sum_{t=1}^m a_t(\tilde{\sigma}^m) \circ \left(b_{t0}(\tilde{\tau}^n) \oplus \sum_{v=1}^n b_{tv}(\tilde{\tau}^n) \circ y_v \right) \\ &= \left(a_0(\tilde{\sigma}^m) \oplus \sum_{t=1}^m a_t(\tilde{\sigma}^m) \circ b_{t0}(\tilde{\tau}^n) \right) \oplus \sum_{v=1}^n \left(\sum_{t=1}^m a_t(\tilde{\sigma}^m) \circ b_{tv}(\tilde{\tau}^n) \right) \circ y_v, \quad (3) \end{aligned}$$

где $\tilde{\sigma}^m = ((\xi_i f_1)(\tilde{\tau}^n), \dots, (\xi_i f_m)(\tilde{\tau}^n))$.

Итак, i -я составляющая функции $\Phi(\tilde{\tau}^n + p^i \tilde{y}^n)$ есть линейная функция в P_p (относительно $\tilde{y}^n \in E_p^n$). Значит, $\Phi(\tilde{x}^n)$ обладает свойством $H_i(p^r)$. Лемма доказана.

Из доказанных лемм вытекает следующее утверждение.

Теорема 1. Для каждого $i = 1, \dots, r-1$ множество $W_i(p^r)$ является замкнутым классом, включающим класс Pol_{p^r} и содержащимся в классе $\mathfrak{M}_{p^r}$.

Замечание. Классы, аналогичные $W_1(p^r)$, ранее рассматривались А. В. Кузнецовым (см. [16, стр. 97]).

Следствие 1. Каждая полиномиальная функция из P_{p^r} обладает любым из свойств $H_i(p^r)$, $i = 1, \dots, r-1$, т.е. справедливо включение

$$\text{Pol}_{p^r} \subseteq \bigcap_{i=1}^{r-1} W_i(p^r).$$

Пусть $p \geq 3$ и $r \geq 2$. Рассмотрим замкнутые классы в P_{p^r}

$$V_{p^r}(l_1, \dots, l_m) = [1, x + y, xy, h_{l_1}^{(1)}(x), \dots, h_{l_m}^{(1)}(x)],$$

где $\emptyset \subseteq \{l_1, \dots, l_m\} \subseteq \{1, \dots, r-1\}$.

Среди этих классов находятся классы $\text{Pol}_{p^r} = V_{p^r}(\emptyset)$ и $\mathfrak{M}_{p^r} = V_{p^r}(1, \dots, r-1)$.

Из леммы 1 вытекает следующее утверждение.

Следствие 2. Для всякого подмножества $L = \{l_1, \dots, l_m\}$ множества $E'_r = \{1, \dots, r-1\}$ справедливо включение

$$V_{p^r}(l_1, \dots, l_m) \subseteq \bigcap_{i \in E'_r \setminus L} W_i(p^r).$$

(Пересечение, взятое по пустому множеству индексов, совпадает с классом $\mathfrak{M}_{p^r}$.)

Классы $V_{p^r}(l_1, \dots, l_m)$ попарно различны и образуют (вместе с классом Pol_{p^r}) решетку (по включению), изоморфную решетке всех подмножеств множества $\{1, \dots, r-1\}$. Ее ширина равна $\binom{r-1}{\lfloor (r-1)/2 \rfloor}$, высота равна $r-1$ и в ней 2^{r-1} элементов.

3. Свойство H'_i

В этом параграфе $p = 2$, $r \geq 3$ и $2 \leq i \leq r-1$. Пусть i фиксировано. Будем говорить, что функция $f(\tilde{x}^n)$ из $W_i(2^r)$ обладает свойством $H'_i(2^r)$, если при всяком $\tau \in E_{2^{i-1}}$ сумма

$$(\theta_i f)(\tau + 2^{i-1} + 2^i y, \dots, \tau + 2^{i-1} + 2^i y) \oplus (\theta_i f)(\tau + 2^i y, \dots, \tau + 2^i y),$$

где $y \in \{0, 1\}$, от y зависит несущественным образом (т. е. может существенно зависеть только от τ). Множество всех функций из $W_i(2^r)$, обладающих свойством $H'_i(2^r)$, обозначим через $W'_i(2^r)$.

Замечание. Легко видеть, что добавление и изъятие фиктивных переменных не нарушает свойства функций, состоящее в их принадлежности множеству $W'_i(2^r)$.

Лемма 4. Пусть

$$f_0(x_1, x_2) \in \{x + y, xy\} \cup \bigcup_{l=1}^{r-1} \{h_l^{(2)}(\tilde{x}^2)\} \subset W_i(2^r), \quad f_1(\tilde{x}^n), f_2(\tilde{x}^n) \in W'_i(2^r),$$

где $i \geq 2$ и $n \geq 1$. Тогда

$$\Phi(\tilde{x}^n) = f_0(f_1(\tilde{x}^n), f_2(\tilde{x}^n)) \in W'_i(2^r).$$

Доказательство. Если $f_0(x_1, x_2) = h_l^{(2)}(\tilde{x}^2)$, $l \neq i$, то утверждение очевидно, ибо $(\theta_i h_l^{(2)})(\tilde{x}^2) \equiv 0$ при $l \neq i$. Рассмотрим далее случай, когда $f_0(x_1, x_2) = x_1 + x_2$ и $f_0(x_1, x_2) = x_1 x_2$. Пусть

$$\varphi(\tau, y) = (\theta_i \Phi)(\tau + 2^{i-1} + 2^i y, \dots, \tau + 2^{i-1} + 2^i y) \oplus (\theta_i \Phi)(\tau + 2^i y, \dots, \tau + 2^i y),$$

где $\tau \in E_{2^{i-1}}$. Так как f_0, f_1 и f_2 принадлежат $W_i(2^r)$, в силу соотношения (3) из доказательства леммы 3

$$\begin{aligned} \varphi(\tau, y) = & \left(a_0(\tilde{\sigma}_1^2) \oplus \sum_{t=1}^2 a_t(\tilde{\sigma}_1^2) \circ b_{t0}(\tau + 2^{i-1}, \dots, \tau + 2^{i-1}) \right) \\ & \oplus \left(\sum_{t=1}^2 a_t(\tilde{\sigma}_1^2) \circ \left(\sum_{v=1}^n b_{tv}(\tau + 2^{i-1}, \dots, \tau + 2^{i-1}) \right) \right) \circ y \\ & \oplus \left(a_0(\tilde{\sigma}_2^2) \oplus \sum_{t=1}^2 a_t(\tilde{\sigma}_2^2) \circ b_{t0}(\tau, \dots, \tau) \right) \\ & \oplus \left(\sum_{t=1}^2 a_t(\tilde{\sigma}_2^2) \circ \left(\sum_{v=1}^n b_{tv}(\tau, \dots, \tau) \right) \right) \circ y, \end{aligned}$$

где

$$\begin{aligned} \tilde{\sigma}_1^2 &= ((\xi_i f_1)(\tau + 2^{i-1}, \dots, \tau + 2^{i-1}), (\xi_i f_2)(\tau + 2^{i-1}, \dots, \tau + 2^{i-1})), \\ \tilde{\sigma}_2^2 &= ((\xi_i f_1)(\tau, \dots, \tau), (\xi_i f_2)(\tau, \dots, \tau)), \\ a_0(\tilde{\sigma}_1^2) &= (\theta_i f_0)(\tilde{\sigma}_1^2), \\ a_1(\tilde{\sigma}_1^2) &= (\theta_i f_0)((\xi_i f_1)(\tau + 2^{i-1}, \dots, \tau + 2^{i-1}) + 2^i, (\xi_i f_2)(\tau + 2^{i-1}, \dots, \tau + 2^{i-1})) \\ &\quad \oplus (\theta_i f_0)(\tilde{\sigma}_1^2), \\ a_2(\tilde{\sigma}_1^2) &= (\theta_i f_0)((\xi_i f_1)(\tau + 2^{i-1}, \dots, \tau + 2^{i-1}), (\xi_i f_2)(\tau + 2^{i-1}, \dots, \tau + 2^{i-1}) + 2^i) \\ &\quad \oplus (\theta_i f_0)(\tilde{\sigma}_1^2), \\ a_0(\tilde{\sigma}_2^2) &= (\theta_i f_0)(\tilde{\sigma}_2^2), \\ a_1(\tilde{\sigma}_2^2) &= (\theta_i f_0)((\xi_i f_1)(\tau, \dots, \tau) + 2^i, (\xi_i f_2)(\tau, \dots, \tau)) \oplus (\theta_i f_0)(\tilde{\sigma}_2^2), \\ a_2(\tilde{\sigma}_2^2) &= (\theta_i f_0)((\xi_i f_1)(\tau, \dots, \tau), (\xi_i f_2)(\tau, \dots, \tau) + 2^i) \oplus (\theta_i f_0)(\tilde{\sigma}_2^2), \\ \sum_{v=1}^n b_{t0}(\tau + 2^{i-1}, \dots, \tau + 2^{i-1}) &= (\theta_i f_t)(\tau + 2^{i-1}, \dots, \tau + 2^{i-1}), \\ \sum_{v=1}^n b_{tv}(\tau + 2^{i-1}, \dots, \tau + 2^{i-1}) &= (\theta_i f_t)(\tau + 2^{i-1} + 2^i, \dots, \tau + 2^{i-1} + 2^i) \\ &\quad \oplus (\theta_i f_t)(\tau + 2^{i-1}, \dots, \tau + 2^{i-1}), \\ b_{t0}(\tau, \dots, \tau) &= (\theta_i f_t)(\tau, \dots, \tau), \\ \sum_{v=1}^n b_{tv}(\tau, \dots, \tau) &= (\theta_i f_t)(\tau + 2^i, \dots, \tau + 2^i) \oplus (\theta_i f_t)(\tau, \dots, \tau). \end{aligned}$$

Для обоснования того, что $\varphi(\tau, y)$ не зависит существенно от y , достаточно показать, что при всяком $\tau \in E_{2^{i-1}}$ справедливо равенство

$$\sum_{t=1}^2 a_t(\tilde{\sigma}_1^2) \circ \left(\sum_{v=1}^n b_{tv}(\tau + 2^{i-1}, \dots, \tau + 2^{i-1}) \right) \oplus \sum_{t=1}^2 a_t(\tilde{\sigma}_2^2) \circ \left(\sum_{v=1}^n b_{tv}(\tau, \dots, \tau) \right) = 0. \quad (4)$$

Так как по условию функции f_1 и f_2 обладают свойством $H_i^!(2^t)$, при $t = 1, 2$ для любого $\tau \in E_{2^{i-1}}$

$$\begin{aligned} (\theta_i f_t)(\tau + 2^{i-1} + 2^i, \dots, \tau + 2^{i-1} + 2^i) \oplus (\theta_i f_t)(\tau + 2^i, \dots, \tau + 2^i) \\ = (\theta_i f_t)(\tau + 2^{i-1}, \dots, \tau + 2^{i-1}) \oplus (\theta_i f_t)(\tau, \dots, \tau). \end{aligned}$$

Следовательно,

$$\sum_{v=1}^n b_{tv}(\tau + 2^{i-1}, \dots, \tau + 2^{i-1}) = \sum_{v=1}^n b_{tv}(\tau, \dots, \tau)$$

и поэтому для доказательства равенства (4) достаточно установить, что для всякого $\tau \in E_{2^{i-1}}$

$$\sum_{t=1}^2 (a_t(\bar{\sigma}_1^2) \oplus a_t(\bar{\sigma}_2^2)) = 0. \quad (5)$$

Пусть $f_0(x_1, x_2) = x_1 + x_2$. Как было показано в доказательстве леммы 1, в этом случае

$$(\theta_i f_0)(\tau_1 + 2^i y_1, \tau_2 + 2^i y_2) = \theta_i(\tau_1 + \tau_2) \oplus y_1 \oplus y_2.$$

Значит,

$$\begin{aligned} a_1(\bar{\sigma}_1^2) \oplus a_1(\bar{\sigma}_2^2) \\ = \theta_i((\xi_i f_1)(\tau + 2^{i-1}, \dots, \tau + 2^{i-1}) + (\xi_i f_2)(\tau + 2^{i-1}, \dots, \tau + 2^{i-1})) \oplus 1 \\ \oplus (\theta_i f_0)(\bar{\sigma}_1^2) \oplus \theta_i((\xi_i f_1)(\tau, \dots, \tau) + (\xi_i f_2)(\tau, \dots, \tau)) \oplus 1 \oplus (\theta_i f_0)(\bar{\sigma}_2^2) = 0. \end{aligned}$$

Аналогично устанавливается, что $a_2(\bar{\sigma}_1^2) \oplus a_2(\bar{\sigma}_2^2) = 0$.

Итак, в случае, когда $f_0(x_1, x_2) = x_1 + x_2$, соотношение (5) справедливо.

Пусть теперь $f_0(x_1, x_2) = x_1 x_2$. Тогда (см. доказательство леммы 1)

$$(\theta_i f_0)(\tau_1 + 2^i y_1, \tau_2 + 2^i y_2) = \theta_i(\tau_1 \tau_2) \oplus ((\theta_0(\tau_1)) \circ y_2) \oplus ((\theta_0(\tau_2)) \circ y_1),$$

а поэтому

$$\begin{aligned} a_1(\bar{\sigma}_1^2) &= \theta_i(((\xi_i f_1)(\tau + 2^{i-1}, \dots, \tau + 2^{i-1}))((\xi_i f_2)(\tau + 2^{i-1}, \dots, \tau + 2^{i-1}))) \\ &\quad \oplus \theta_0((\xi_i f_1)(\tau + 2^{i-1}, \dots, \tau + 2^{i-1})) \cdot 0 \\ &\quad \oplus \theta_0((\xi_i f_2)(\tau + 2^{i-1}, \dots, \tau + 2^{i-1})) \cdot 1 \\ &\quad \oplus \theta_i(((\xi_i f_1)(\tau + 2^{i-1}, \dots, \tau + 2^{i-1}))((\xi_i f_2)(\tau + 2^{i-1}, \dots, \tau + 2^{i-1}))) \\ &= \theta_0((\xi_i f_2)(\tau + 2^{i-1}, \dots, \tau + 2^{i-1})) = (\theta_0 f_2)(\tau + 2^{i-1}, \dots, \tau + 2^{i-1}), \\ a_1(\bar{\sigma}_2^2) &= \theta_i(((\xi_i f_1)(\tau, \dots, \tau))((\xi_i f_2)(\tau, \dots, \tau))) \oplus \theta_0((\xi_i f_2)(\tau, \dots, \tau)) \cdot 1 \\ &\quad \oplus \theta_i(((\xi_i f_1)(\tau, \dots, \tau))((\xi_i f_2)(\tau, \dots, \tau))) \\ &= \theta_0((\xi_i f_2)(\tau, \dots, \tau)) = (\theta_0 f_2)(\tau, \dots, \tau). \end{aligned}$$

Аналогично, $a_2(\bar{\sigma}_1^2) = (\theta_0 f_1)(\tau + 2^{i-1}, \dots, \tau + 2^{i-1})$ и $a_2(\bar{\sigma}_2^2) = (\theta_0 f_1)(\tau, \dots, \tau)$.

Так как (см. доказательство леммы 3) при $i \geq 2$

$$(\theta_0 f_t)(\tau + 2^{i-1}, \dots, \tau + 2^{i-1}) = (\theta_0 f_t)(\tau, \dots, \tau),$$

где $t = 1, 2$, то $a_t(\bar{\sigma}_1^2) = a_t(\bar{\sigma}_2^2)$.

Следовательно, соотношение (5) справедливо и в случае, когда $f_0(x_1, x_2) = x_1 x_2$. Лемма доказана.

Лемма 5. *Функции 1 и x принадлежат множеству $W'_i(2^r)$, а $h_i^{(1)}(x) \notin W'_i(2^r)$.*

Доказательство. Если $f(x) = 1$, то $(\theta_i f)(x) \equiv 0$, и утверждение очевидно. Пусть $f(x) = x$. Тогда

$$(\theta_i f)(\tau + 2^{i-1} + 2^i y) \oplus (\theta_i f)(\tau + 2^i y) = y \oplus y = 0.$$

Значит, $x \in W'_i(2^r)$. Рассмотрим теперь функцию $h_i^{(1)}(x)$. Так как $(\theta_i h_i^{(1)})(0) = 1$ и

$$(\theta_i h_i^{(1)})(2^{i-1}) = (\theta_i h_i^{(1)})(2^i) = (\theta_i h_i^{(1)})(2^{i-1} + 2^i) = 0,$$

справедливо равенство

$$(\theta_i h_i^{(1)})(2^{i-1} + 2^i y) \oplus (\theta_i h_i^{(1)})(2^i y) = 1 \oplus y,$$

т.е. эта функция существенно зависит от y . Следовательно, $h_i^{(1)}(x) \notin W'_i(2^r)$. Лемма доказана.

Из лемм 4 и 5 вытекает следующее утверждение.

Теорема 2. *Для всякого i , $2 \leq i \leq r-1$, справедливы включения*

$$\left[\{1, x + y, xy\} \cup \bigcup_{l=1, l \neq i}^{r-1} \{h_l^{(2)}(\tilde{x}^2)\} \right] \subseteq [W'_i(2^r)] \subsetneq W_i(2^r),$$

причем $h_i^{(1)}(x) \notin [W'_i(2^r)]$.

(Квадратные скобки означают здесь замыкание соответствующего множества.)

Рассмотрим замкнутые классы в P_{2^r} , $r \geq 3$,

$$V_{2^r}(l_1, \dots, l_m; s_1, \dots, s_t) = [1, x + y, xy, h_{l_1}^{(1)}(x), \dots, h_{l_m}^{(1)}(x), h_{s_1}^{(2)}(\tilde{x}^2), \dots, h_{s_t}^{(2)}(\tilde{x}^2)],$$

где

$$\emptyset \subseteq \{l_1, \dots, l_m\} \subseteq \{2, \dots, r-1\},$$

$$\emptyset \subseteq \{s_1, \dots, s_t\} \subseteq \{1, \dots, r-1\},$$

$$\{l_1, \dots, l_m\} \cap \{s_1, \dots, s_t\} = \emptyset.$$

Среди этих классов находятся классы $\text{Pol}_{2^r} = V_{2^r}(\emptyset, \emptyset)$ и $\mathfrak{M}_{2^r} = V_{2^r}(\emptyset; 1, \dots, r-1)$.

Из следствия 2 и теоремы 2 легко получается следующее утверждение.

Теорема 3. *Пусть $L = \{l_1, \dots, l_m\}$ и $S = \{s_1, \dots, s_t\}$ — подмножества множеств $E_r'' = \{2, \dots, r-1\}$ и $E_r' = \{1, \dots, r-1\}$ соответственно. Тогда справедливо включение*

$$V_{2^r}(l_1, \dots, l_m; s_1, \dots, s_t) \subseteq \bigcap_{i \in E_r'' \setminus S} W_i(2^r) \cap \bigcap_{j \in E_r' \setminus (L \cup S)} [W'_j(2^r)].$$

Рис. 1.

(Пересечение, взятое по пустому множеству индексов, совпадает с классом $\mathfrak{M}_{2^r}$.)

Следствие 3. Разным допустимым парам $(L; S)$, т.е. таким, что $L \cap S = \emptyset$, соответствуют разные классы $V_{2^r}(l_1, \dots, l_m; s_1, \dots, s_t)$.

Замечание. Нетрудно показать, что

$$h_1^{(1)}(x-2) + \sum_{i=2}^{r-1} \sum_{l=2^{i-1}}^{2^i-1} h_i^{(1)}(x-2l) = xh_0^{(1)}(x). \quad (6)$$

Но так как $h_0^{(1)}(x) = 1 - x^{2^{r-1}} \in \text{Pol}_{2^r}$ и $h_1^{(1)}(x) \notin \text{Pol}_{2^r}$ (см. [1]), то, учитывая (6), находим, что справедливы строгие включения

$$\text{Pol}_{2^r} \subset V_{2^r}(1; \emptyset) = [1, x + y, xy, h_1^{(1)}(x)] \subset V_{2^r}(2, \dots, r-1; \emptyset).$$

Класс $V_{2^r}(1; \emptyset)$ отличен от каждого из классов $V_{2^r}(L; S)$, где $\emptyset \subseteq L \subseteq E_r''$, $\emptyset \subseteq S \subseteq E_r'$ и $L \cap S = \emptyset$, и все эти классы образуют решетку (по включению), состоящую из $2 \cdot 3^{r-2} + 1$ элементов. Ее ширина $\binom{r-1}{\lfloor (r-1)/2 \rfloor}$, а высота равна $2r - 2$.

На рис. 1 изображена эта решетка для случая $r = 3$.

Список литературы

1. Гаврилов Г. П. О надструктуре класса полиномов в многозначных логиках. *Дискретная математика* (1996) **8**, №3, 90–97.

2. Hermite Ch. Sur les fonctions de sept lettres. *C. R. Acad. Sci. Paris* (1863) **57**, 750–757.
3. Kempner A. J. Polynomials and their residue systems. *Trans. Amer. Math. Soc.* (1921) **22**, 240–288.
4. Bernstein B. A. Modular representations of finite algebras. *Proc. Intern. Math. Congress, Vol.1.* Univ. Toronto Press, Toronto, 1928, 207–216.
5. Litzinger M. A basis for residual polynomials in n variables. *Trans. Amer. Math. Soc.* (1935) **37**, 216–225.
6. Nöbauer W. Über Gruppen von Restklassen nach Restpolynomidealen. *Sitzungsber. Österr. Akad. Wiss. Abt. II* (1953) **162**, 207–233.
7. Carlitz L. Functions and polynomials (mod p^n). *Acta Arithmetica* (1964) №9, 66–78.
8. Keller G., Olson F. R. Counting polynomial (mod p^n). *Duke Math. J.* (1968) **35**, №4, 835–838.
9. Айзенберг Н. Н., Семйон И. В., Циткин А. И. Полиномиальные представления логических функций. *Автоматика и вычисл. техника* (1971) №2, 6–13.
10. Айзенберг Н. Н., Семйон И. В., Циткин А. И. Мощность класса функций k -значной логики от n переменных, представимых полиномами по модулю k . В кн: *Многоустойчивые элементы и их применение*. Сов. радио, Москва, 1971, с.78–83.
11. Айзенберг Н. Н., Семйон И. В. Некоторые критерии представимости функций k -значной логики полиномами по модулю k . В кн: *Многоустойчивые элементы и их применение*. Сов. радио, Москва, 1971, с.84–88.
12. Singmaster D. On polynomial functions (mod m). *J. Number Theory* (1974) **6**, №5, 345–352.
13. Rosenberg I. G. Polynomial functions over finite rings. *Glasnik Matematički* (1975) **10**, №1, 25–33.
14. Мещанинов Д. Г. О вторых p -разностях функций p^α -значной логики. *Дискретная математика* (1992) **4**, №4, 131–139.
15. Мещанинов Д. Г. Метод построения полиномов для функций k -значной логики. *Дискретная математика* (1995) **7**, №3, 48–60.
16. Яблонский С. В. Функциональные построения в k -значной логике. *Труды Матем. ин-та АН СССР* (1958) **51**, 5–142.
17. Черепов А. Н. Описание структуры замкнутых классов в P_k , содержащих класс полиномов. *Проблемы кибернетики* (1983) **40**, 5–18.
18. Черепов А. Н. Надструктура класса сохранения отношений сравнения при $k = p^m$. В кн: *Моделирование и оптимизация вычислительных систем и процессов*. Ярослав. гос. ун-т, Ярославль, 1988, с.61–65.
19. Мещанинов Д. Г. О полиномиальной реализации функций k -значной логики. Деп. ВИНТИ 23.10.87, №7441–В87.
20. Мещанинов Д. Г. Некоторые условия представимости функций из P_k полиномами по модулю k . *Докл. АН СССР* (1988) **299**, №1, 50–53.
21. Мещанинов Д. Г. О некоторых свойствах надструктуры класса полиномов в P_k . *Матем. заметки* (1988) **44**, №5, 673–681.
22. Мещанинов Д. Г. Перестановочные представления функций k -значной логики. *Вестн. МГУ. Сер. 15. Вычисл. математика и кибернетика* (1988) №3, 61–66.
23. Ремизов А. Б. О надструктуре замкнутого класса полиномов по модулю k . *Дискретная математика* (1989) **1**, №1, 3–15.