А. А. Часовских, Проблема полноты для класса линейно-автоматных функций, *Дискрет. матем.*, 2015, том 27, выпуск 2, 134–151

DOI: 10.4213/dm1330

Дискретная математика

том 27 выпуск 2 * 2015

УДК 519.716.3 DOI 10.4213/dm1330

Проблема полноты для класса линейно-автоматных функций

© 2015 г. А. А. Часовских*

Рассматриваются классы линейно-автоматных функций над конечными полями с операциями композиции (суперпозиции и обратной связи). Для этих классов получен алгоритм проверки полноты конечных систем. Таким образом, обобщается результат, известный для классов линейно-автоматных функций над простыми конечными полями.

Ключевые слова: конечный автомат, линейно-автоматная функция, операции композиции, операции суперпозиции, обратная связь, проблема полноты, критерий полноты, сумматор, задержка.

1. Постановка задачи. Необходимое условие K-полноты

Зафиксируем простое число p и натуральное число m. Через k обозначим число p^m, а через $E_k[\xi]$ обозначим множество всех многочленов от переменной ξ над полем E_k. Для множества всех многочленов из $E_k[\xi]$ с ненулевым свободным членом будем использовать обозначение $E'_k[\xi]$. Поле отношений многочленов из $E_k[\xi]$ обозначаем $E_k(\xi)$, а его подкольцо

$$\left\{\frac{u(\xi)}{v(\xi)} \mid u(\xi) \in E_k[\xi],\ v(\xi) \in E'_k[\xi]\right\}$$

будем обозначать $E'_k(\xi)$. Множество всех формальных степенных рядов по переменной ξ с коэффициентами из E_k будем обозначать $R_k(\xi)$.

Пусть $n \in \mathbb{N}$. Отображение $f(x_1, x_2, \ldots, x_n)$ из $R_k^n(\xi)$ в $R_k(\xi)$ называется линейно-автоматной функцией (л.-а. функцией) над E_k, если найдутся такие μ_i, $\mu_i \in E'_k(\xi)$, $i = 0, 1, \ldots, n$, что для любых α_i, $\alpha_i \in R_k(\xi)$, $i = 1, 2, \ldots, n$, выполнено равенство

$$f(\alpha_1, \alpha_2, \ldots, \alpha_n) = \sum_{i=1}^{n} \mu_i \alpha_i + \mu_0, \tag{1}$$

где операции "$+$"и "$\cdot$"индуцированы операциями в E_k. Поэтому л.-а. функция $f(x_1, x_2, \ldots, x_n)$ задается выражением $\sum_{i=1}^n \mu_i x_i + \mu_0$.

Как показано в [2], л.-а. функция реализуется линейной последовательной машиной. При этом ряд α_i, $\alpha_i = \sum_{i=0}^{\infty} \alpha_i(t)\xi^t$, соответствует последовательности $\alpha_i(0)$,

*Место работы: МГУ им. М. В. Ломоносова, e-mail: chasovskikh@mail.ru

$\alpha_i(1), \ldots$, подаваемой на i-й вход машины, а параметр t определяет момент времени подачи сигнала $\alpha_i(t)$. Множество всех л.-а. функций над E_k обозначим $\mathfrak{L}_k$.

Приведем примеры л.-а. функций из $\mathfrak{L}_k$ (см. [2]).

(1) Сумматор от n переменных: $x_1 + x_2 + \ldots + x_n$, $n \in \mathbb{N}$.

(2) Усилители: $a \cdot x$, $a \in E_k \setminus \{0\}$.

(3) Константа: μ, $\mu \in E'_k(\xi)$.

(4) Задержка с начальным состоянием a, $a \in E_k$: $\xi \cdot x + a$.

В классе $\mathfrak{L}_k$ рассмотрим операторы замыкания S и K по операциям суперпозиции и композиции соответственно [4; стр. 155].

Пусть $M \subseteq \mathfrak{L}_k$. Множество M называется K-полным, если $K(M) = \mathfrak{L}_k$. Множество M называется K-базисом, если оно K-полно и $K(M \setminus \{f\}) \neq \mathfrak{L}_k$ для любой $f \in M$.

Пусть

$$B = \begin{cases} \{x_1 + x_2,\ \xi \cdot x,\ 1\}, & \text{если} \quad m = 1 \\ \{x_1 + x_2,\ a \cdot x,\ \xi \cdot x,\ 1\} \ |a - & \\ \text{примитивный элемент [6] поля } E_k, & \text{если} \quad m > 1. \end{cases}$$

Нетрудно доказать следующее утверждение.

Лемма 1. *Множество л.-а. функций B является K-базисом в $\mathfrak{L}_k$.*

Цель настоящей работы — построить алгоритм, позволяющий по заданному конечному множеству л.-а. функций проверять, является ли оно K-полным.

Через $\mu(0)$ будем обозначать свободный член ряда $\mu(\xi)$, $\mu(\xi) \in R_k(\xi)$.

Рассмотрим следующие множества л.-а. функций.

Пусть $s \in E_k$,

$$\begin{aligned} T_s = \Big\{ & f(x_1, x_2, \ldots, x_n) \ \mid\ n \in \mathbb{N},\ f \in \mathfrak{L}_k,\ \text{из} \\ & f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0 \ \text{следует} \\ & \sum_{i=1}^{n} \mu_i(0) \cdot s + \mu_0(0) = s \Big\}. \end{aligned}$$

Таким образом, T_s — множество всех л.-а. функций, сохраняющих число s в начальный момент времени.

Далее, положим

$$\begin{aligned} V_1 = \big\{ & f(x_1, x_2, \ldots, x_n) \ \mid\ n \in \mathbb{N},\ f \in \mathfrak{L}_k, \\ & f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0, \\ & \text{среди чисел } \mu_i(0),\ i = 1, 2, \ldots, n, \\ & \text{не более одного отличного от нуля} \big\}, \end{aligned}$$

т.е. V_1 — множество всех л.-а. функций, существенно зависящих в начальный момент не более чем от одной переменной.

Множество M, $M \subseteq \mathfrak{L}_k$, называется K-замкнутым классом, если выполнено равенство $M = K(M)$.

Как нетрудно видеть, л.-а. функции, рассматриваемые в этой работе, в первый момент времени реализуют квазилинейные функции над полем E_k [8], [9]. В работе [9] были определены все замкнутые подклассы класса L_k всех квазилинейных функций, не содержащиеся в классе одноместных функций. Это множество классов квазилинейных функций обозначим $J_{k,0}$.

Каждому классу Θ, $\Theta \in J_{k,0}$, сопоставим класс Θ' всех л.-а. функций, каждая из которых в начальный момент времени реализует функцию из Θ. Положим:

$$J' = \{\ \Theta' \ \mid\ \Theta \in J_{k,0}\ \} \cup V_1.$$

Для каждого s, $s \in E_k$, выполнено: $T_s \in J'$.

Используя результат работы [9], несложно доказать следующее утверждение.

Теорема 1. *Каждый элемент множества J'_k является K-замкнутым классом, не совпадающим с $\mathfrak{L}_k$.*

Пусть л.-а. функция $f\,(x_1, x_2, \ldots, x_n)$ определена равенством (1). Тогда положим:

$$U(f) = \{\mu_i \ \mid\ i = 1, 2, ..., n\}\,,$$

а для множества л.-а. функций M

$$U(M) = \cup_{f \in M} U(f).$$

Таким образом, $U(M) \subseteq E'_k(\xi)$.

Теорема 2. *Для множества M, $M \subseteq \mathfrak{L}_k$, равенство*

$$K(M) = \mathfrak{L}_k \tag{2}$$

выполнено в точности тогда, когда имеют место следующие свойства:
для любого $\Theta \in J'_k$

$$M \not\subseteq \Theta, \tag{3}$$

$$U(K(M)) = E'_k(\xi). \tag{4}$$

Для доказательства полноты множества M, удовлетворяющего условиям (3) и (4), нам понадобится вспомогательное утверждение.

Лемма 2. *Если для некоторого M, $M \subseteq \mathfrak{L}_k$, выполнены условия (3) и (4), то:*

$$x_1 + x_2 + \ldots + x_{p+1} \in K(M), \tag{5}$$

для любого μ, $\mu \in E'_k(\xi)$, в $K(M)$ содержится функция

$$x_1 + \mu \cdot x_2 + \mu \cdot x_3 + \ldots + \mu \cdot x_{p+1}, \tag{6}$$

в $K(M)$ содержатся такие константы ν_0 и ν'_0, что

$$\nu_0(0) = 0, \quad \nu'_0(0) \neq 0. \tag{7}$$

Доказательство. Рассмотрим множество M, $M \subseteq \mathfrak{L}_k$, обладающее свойствами (3) и (4).

Тогда найдется л.-а. функция $f\left(x_1, x_2, \ldots, x_n\right)$, $f \in M \setminus V_1$. Для некоторых μ_i, $\mu_i \in E'_k(\xi)$, $i = 0, 1, \ldots, n$, имеет место равенство (1). Не ограничивая общности рассуждений, будем предполагать, что $\mu_i(0) \neq 0$, $i = 1, 2$. Найдутся такие л.-а. функции g_i, $g_i \in K(M)$, $i = 1, 2$, что $\mu_i^{-1} \in U(g_i)$. Из функции g_i, используя операции переименования и отождествления переменных, получим л.-а. функцию $g'_i(x_i, x_3)$, $g'_i(x_i, x_3) = \mu_i^{-1} \cdot x_i + g''_i(x_3)$, $i = 1, 2$. Тогда, обозначив л.-а. функцию $f\left(g'_1(x_1, x_3), g'_2(x_2, x_3), x_3, \ldots, x_3\right)$ через $h\left(x_1, x_2, x_3\right)$, для некоторых μ'_i, $i = 0, 1$, имеем: $h\left(x_1, x_2, x_3\right) = x_1 + x_2 + \mu'_1 \cdot x_3 + \mu'_0$. Имеет место равенство

$$h\left(x_1, h\left(x_2, \ldots h\left(x_p, x_{p+1}, x\right), \ldots x\right), x\right) = x_1 + x_2 + \ldots + x_{p+1}.$$

Поэтому включение (5) доказано.

Далее, для каждого μ, $\mu \in E'_k(\xi)$, в $K(M)$ содержится такая л.-а. функция $f_\mu(x, x_1)$, что для некоторых μ_1 и μ_0 из $E'_k(\xi)$ выполнено

$$f_\mu(x, x_1) = \mu \cdot x + \mu_1 \cdot x_1 + \mu_0.$$

Имеет место равенство

$$x_1 + f_\mu(x_2, x) + f_\mu(x_3, x) + \ldots + f_\mu(x_{p+1}, x) = x_1 + \mu \cdot x_2 + \mu \cdot x_3 + \ldots + \mu \cdot x_{p+1},$$

доказывающее утверждение (6).

Из предположения (3) следует, что в $K(M)$ содержатся функции $\tilde{\eta}_0$ и $\tilde{\eta}'_0$, реализующие в первый момент времени константы 0 и 1, соответственно. Отождествляя переменные каждой из этих функций, затем применяя операцию обратной связи к полученным одноместным функциям, получаем константы η_0 и η'_0, удовлетворяющие (7). Лемма доказана.

Доказательство теоремы. Пусть выполнено (2). Тогда свойство (3) следует из теоремы 1, а справедливость (4) очевидна.

Пусть для множества M, $M \subseteq \mathfrak{L}_k$, выполнены условия (3) и (4). Согласно лемме 2, в $K(M)$ содержатся такие константы ν_0 и ν'_0, что $\nu_0(0) = 0$, $\nu'_0(0) \neq 0$. Тогда для некоторых многочленов $u(\xi)$, $u'(\xi)$, $v(\xi)$, $v'(\xi)$ из $E_k[\xi]$ имеют место равенства

$$\nu_0 = \frac{\xi \cdot u(\xi)}{1 + \xi \cdot v(\xi)},\ \nu'_0 = \frac{-1 + \xi \cdot u'(\xi)}{v'(\xi)}.$$

Справедливо тождество

$$\left(1 - \xi \cdot u'(\xi)\right)\left(1 + \xi \cdot v(\xi)\right)\nu_0 + \xi \cdot u(\xi) v'(\xi) \nu'_0 = 0.$$

Через $u_1(\xi)$ и $u_2(\xi)$ обозначим многочлены $\xi\left(v(\xi) - u'(\xi) - \xi v(\xi) u'(\xi)\right)$ и $\xi u(\xi) v'(\xi)$, соответственно. Имеем тождество:

$$\nu_0 + u_1(\xi)\nu_0 + u_2(\xi)\nu'_0 = 0,$$

причем $u_i(\xi) \in \{\xi\} \cdot E_k[\xi]$, $i = 1, 2$.

Из (6) следует: $x_1 + u_i \cdot x_2 + u_i \cdot x_3 + \ldots + u_i \cdot x_{p+1} \in K(M)$, $i = 1, 2$. Используя эти л.-а. функции, операции подстановки, переименования и отождествления переменных, получаем л.-а. функцию $f\left(x_1, x_2, x_3\right) = x_1 + u_1 \cdot x_1 + u_2 \cdot x_2 - \left(u_1 + u_2\right) x_3$. Применяя операцию обратной связи к единственной переменной функции $f(\nu_0, \nu_0', x)$, получим константу 0.

Далее используем (5). Подставляя константу 0 вместо переменных $x_3, x_4, \ldots, x_{p+1}$ сумматора $x_1 + x_2 + \ldots + x_{p+1}$, получим сумматор $x_1 + x_2$. Для любого μ, $\mu \in E_k'(\xi)$, выполнено (6). Поэтому $\mu \cdot x = 0 + \mu \cdot x + \mu \cdot 0 + \ldots + \mu \cdot 0 \in K(M)$. Значит, $\xi \cdot x \in K(M)$ и $a \cdot x \in K(M)$ для любого a, $a \in E_k$. Далее, $(\nu_0')^{-1}(x) \in K(M)$, поэтому $1 = (\nu_0')^{-1}(\nu_0') \in K(M)$. Отсюда и из леммы 1 следует равенство (2).

Теорема 2 доказана.

В соответствии с теоремой 2 проверка K-полноты конечной системы M, $M \subseteq \mathfrak{L}_k$, сводится к проверке свойств (3) и (4). Проверка свойства (3) не вызывает затруднений, поэтому в дальнейшем будет построен алгоритм проверки свойства (4).

Замыкание множества M, $M \subseteq E_k'(\xi)$, по операциям сложения и умножения будем обозначать $S^1(M)$. В кольце $E_k'(\xi)$ помимо операций сложения и умножения будем рассматривать также операцию "Об". Для элементов μ_1 и μ_2 из $E_k'(\xi)$ значение Об(μ_1, μ_2) определено в точности тогда, когда $\mu_2(0) = 0$. Если последнее равенство спрведливо, то

$$\text{Об}\,(\mu_1, \mu_2) = \frac{\mu_1}{1 - \mu_2}.$$

Замыкание множества M, $M \subseteq E_k'(\xi)$, по операциям сложения, умножения и операции Об обозначаем $K^1(M)$.

В соответствии с [4] множество M, $M \subseteq E_k'(\xi)$, называется K^1-замкнутым, если

$$K^1(M) = E_k'(\xi).$$

Следуя рассуждениям, приведенным в [7], можно убедиться в справедливости включения

$$U(K(M)) \subseteq K^1(U(M)). \tag{8}$$

Поэтому равенство

$$K^1(U(M)) = E_k'(\xi) \tag{9}$$

является необходимым условием K-полноты множества M, $M \subseteq \mathfrak{L}_k$. В дальнейшем будет найден алгоритм проверки K^1-полноты конечных подмножеств кольца $E_k'(\xi)$, которое, что доказывается с использованием рассуждений из [7], изоморфно классу одноместных линейно-автоматных функций, сохраняющих нулевую последовательность.

2. Класс одноместных линейно-автоматных функций, сохраняющих нулевую последовательность

Сначала рассмотрим свойства некоторых полей.

В конечном поле E_k,

$$E_k = \{d_0 + d_1 z + \ldots + d_{m-1} z^{m-1} \mid d_i \in E_p,\ i = 0, 1, \ldots, m-1\},$$

введены операции сложения и умножения по модулю некоторого неприводимого над E_p многочлена степени m.

Пусть $\eta \in E_k(\xi)$. Через $E_p(\eta)$ обозначим поле, получаемое простым трансцендентным расширением [1; стр. 141] поля E_p элементом η.

Пусть $M \subseteq E_k(\xi)$. Через $E_p(M)$ обозначим поле, получаемое расширением поля E_p элементами множества M.

Рассмотрим поле $E_k(\xi)$. Если $M \subseteq E_k(\xi)$ и $M \setminus E_k \neq \varnothing$, то найдется η, $\eta \in M \setminus E_k$, для которого имеем конечную башню полей: $E_p(\eta) \subset E_k(\eta) \subset E_k(\xi)$ (см. [5; стр. 185-187]).

Поле $E_k(\eta)$ — векторное пространство над полем $E_p(\eta)$ с базисом $\left\{z^0, z^1, \ldots, z^{m-1}\right\}$.

Обозначим через s степень дроби η по переменной ξ. Поле $E_k(\xi)$ — векторное пространство над полем $E_k(\eta)$ размерности s, с базисом $\left\{\xi^0, \xi^1, \ldots, \xi^{s-1}\right\}$.

Поэтому множество

$$\left\{z^i \xi^j \ \mid \ i = 0, 1, \ldots, m-1, j = 0, 1, \ldots, s-1\right\}$$

является базисом векторного пространства $E_k(\xi)$ над полем $E_p(\eta)$ [3; стр. 77].

Положим $M^1 = M$ и $M^i = M^{i-1} * M \cup M^{i-1}$ для любого i, $i \in \mathbb{N}$, $i > 1$.

Лемма 3. *Поле $E_p(M)$ как векторное пространство над полем $E_p(\eta)$ порождается множеством M^{sm}.*

Доказательство. Если для некоторого натурального i справедливо

$$\dim_{E_p(\eta)} M^i = \dim_{E_p(\eta)} M^{i+1},$$

то для любого натурального j, $j \geqslant i$, имеем:

$$\dim_{E_p(\eta)} M^i = \dim_{E_p(\eta)} M^j.$$

Так как $\dim_{E_p(\eta)} M^i \leqslant ms$, то

$$\dim_{E_p(\eta)} M^{ms} = \dim_{E_p(\eta)} E_p(M).$$

Лемма доказана.

Следствие 1. *Равенство*

$$E_p(M) = E_k(\xi) \tag{10}$$

справедливо в точности тогда, когда

$$\dim_{E_p(\eta)} M^{ms} = ms. \tag{11}$$

Лемма 4. *Пусть $M \subseteq E'_k(\xi)$, $E_p(M) = E_k(\xi)$. Тогда для некоторого μ, $\mu \in E'_k(\xi) \setminus \{0\}$, и любого a, $a \in E_k$, имеет место включение*

$$\{a \cdot \mu, \ a \cdot \xi\mu\} \subset S^1(M). \tag{12}$$

Доказательство. Пусть $M \subseteq E'_k(\xi)$, $E_p(M) = E_k(\xi)$. Тогда в $E'_k(\xi) \setminus \{0\}$ найдутся μ_1 и μ_2, что

$$\{\mu_1, \ z \cdot \mu_1, \ \mu_2, \ \xi \cdot \mu_2\} \subset S^1(M).$$

Положим $\mu = (\mu_1\mu_2)^{m-1}$. Тогда для любого i, $i = 0, 1, \ldots, m-1$, справеливы включения

$$z^i \cdot \mu \in S^1(M)$$

и

$$z^i \cdot \xi \cdot \mu \in S^1(M).$$

Отсюда, для любого a, $a \in E_k$, используя операцию сложения, получаем включение (12).

Лемма доказана.

Используя рассуждения из [7], несложно доказать следующую лемму.

Лемма 5. *Для любого* M, $M \subseteq E'_k(\xi)$, *и для любого* μ, $\mu \in K^1(M)$, *найдутся такие* μ_i, $\mu_i \in S^1(M)$, $i = 1, 2$, *что* $\mu = \text{Об}(\mu_1, \mu_2)$.

Пусть $\mu \in E'_k(\xi)$, $\mu = \frac{u}{v}$, $\deg u \leqslant \deg v$. Тогда для некоторых s, a, a', b, b', u', v', $s \in \mathbb{N}$, $a, a' \in E_k$, $b, b' \in E_k \setminus \{0\}$, $u', v' \in E_k[\xi]$, $\deg u' < s-1$, $\deg v' < s-1$, имеет место равенство

$$\mu = \frac{a + \xi u' + a'\xi^s}{b + \xi v' + b'\xi^s}.$$

Через $\Psi_0(\mu)$ обозначим пару $\left(\frac{a}{b}, \frac{a'}{b'}\right)$ элементов поля E_k. Нетрудно видеть, что пара $\Psi_0(\mu)$ определяется по μ однозначно, потому что сохраняется после умножения числителя и знаменателя дроби μ на один и тот же, не делящийся на ξ, многочлен.

Если $M \subseteq E'_k(\xi)$, то $\Psi_0(M) = \{\Psi_0(\mu) \mid \mu \in M\}$.

Положим

$$M_0^{(1)} = \left\{\mu \mid \mu \in E'_k(\xi),\ \mu = \frac{u}{v},\ \deg u \leqslant \deg v\right\}.$$

Лемма 6. *Пусть* $M \subseteq M_0^{(1)}$. *Соотношение*

$$K^1(M) \nsubseteq M_0^{(1)} \tag{13}$$

выполнено в точности тогда, когда найдется такое b, $b \in E_k \setminus \{0\}$, *что*

$$(0, b) \in \Psi_0(S^1(M)). \tag{14}$$

Доказательство. Если $M \subseteq M_0^{(1)}$, то $S^1(M) \subseteq M_0^{(1)}$. Поэтому из (13) и леммы 5 вытекает, что найдутся такие μ_j, $\mu_j \in S^1(M)$, $j = 1, 2$, что $\text{Об}\,(\mu_1, \mu_2) \notin M_0^{(1)}$. Тогда для некоторого b, $b \in E_k \setminus \{0\}$, выполнено: $\Psi_0\,(\mu_2) = (0, b)$, откуда вытекает (14).

Обратно, пусть выполнено (14) и μ, $\mu \in S^1(M)$, таково, что для некоторого b, $b \in E_k \setminus \{0\}$, имеем $\Psi_0(\mu) = (0, b)$. Тогда для дроби μ', $\mu' = \frac{u'}{v'}$, $\mu' = \text{Об}\left(\mu, \mu^{k-1}\right)$, имеем $\deg u' > \deg v'$. Поэтому (13) выполнено.

Лемма доказана.

На множестве E_k^2 пар чисел поля E_k будем рассматривать операции сложения и умножения, которые определяются покомпонентно:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)\,,$$

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2)\,.$$

Замыкание множества M, $M \subseteq E_k^2$, по операциям сложения и умножения обозначим $S(M)$.

Нетрудно видеть, что $\Psi_0(S^1(M)) = S(\Psi_0(M))$.

Учитывая, что множество, состоящее из всех неприводимых в $E_k[\xi]$ приведенных многочленов, счетно [6], упорядочим эти многочлены некоторым образом: $p_1(\xi), p_2(\xi), \ldots$ так, что $p_1(\xi) = \xi$.

Положим

$$M_i^{(1)} = \left\{\mu \mid \mu \in E'_k(\xi),\ \mu = \frac{u}{v},\ (v, p_i) = 1\right\},$$

$i = 2, 3, \ldots$. Пусть $\mu \in M_i^{(1)}$. Тогда в $E_k[\xi]$ найдутся такие многочлены u', u'', v', что $\deg u' \leqslant \deg p_i$ и

$$\mu = \frac{u' + \xi p_i u''}{1 - \xi p_i v'}.$$

Через $\Psi_i(\mu)$ обозначим пару $(\mu(0), u')$.

Нетрудно видеть, что $\mu(0) = u'(0)$.

Лемма 7. *Пусть для некоторого i, $i \in \{2, 3, \dots\}$, имеет место включение $M \subseteq M_i^{(1)}$. Соотношение*

$$K^1(M) \nsubseteq M_i^{(1)} \tag{15}$$

выполнено в точности тогда, когда в $\Psi_i(S^1(M))$ найдется пара $(0, v)$ с $v \neq 0$.

Доказательство. Пусть $M \subseteq M_i^{(1)}$ для некоторого i, $i \in \mathbb{N}$, и выполнено (15). Тогда по лемме 5 найдутся такие μ_j, $\mu_j \in S^1(M)$,

$$\mu_j = \frac{u'_j + \xi p_i u''_j}{1 - \xi p_i v'_j},$$

$\deg u'_j \leqslant \deg p_i$, $j = 1, 2$, что Об$\,(\mu_1, \mu_2) \notin M_i^{(1)}$. Равенство нулю числа $u'_2(0)$ следует из возможности применения операции Об к паре μ_1, μ_2. Неравенство $u'_2 \neq 0$ получаем ввиду того, что p_i делит многочлен $1 - \xi p_i v'_2 - u'_2 - \xi p_i u''_2$.

В обратную сторону. Пусть $M \subseteq M_i^{(1)}$ и найдется такая μ, $\mu \in S^1(M)$, что $\Psi_i(\mu)$ имеет нулевую первую компоненту и ненулевую вторую. Тогда для некоторого натурального числа T числитель дроби $1 - \mu^T$, предствленной в несократимом виде, делится на p_i. Поэтому Об$\,\left(\mu, \mu^T\right) \notin M_i^{(1)}$.

Лемма доказана.

Для некоторого целого неотрицательного числа τ множество M, $M \subseteq E'_k(\xi)$, назовем τ-предельным, если

$$\xi^\tau E'_k(\xi) \subseteq K^1(M). \tag{16}$$

Множество M назовем предельным, если найдется τ, для которого оно является τ-предельным.

Лемма 8. *Пусть $M \subseteq E'_k(\xi)$. Множество M являетя предельным в точности тогда, когда имеет место условие* (10)*, а также для любого i, $i = 0, 2, 3, \dots$, из $M \subseteq M_i^{(1)}$ следует* (15).

Доказательство. Пусть множество M является предельным. Тогда для некоторого натурального τ выполнено включение (16). Поэтому множество M',

$$M' = \left\{\xi^\tau,\ a \cdot \xi^\tau,\ \xi^{\tau+1} \mid a \in E_k\right\},$$

содержится в $K^1(M)$.

Нетрудно видеть, что множество M'',

$$M'' = \{a,\ \xi \mid a \in E_k\},$$

содержится в $E_p\,(M')$. Далее из соотношения

$$E_k(\xi) = E_p\,(M'') \subseteq E_p(M) \subseteq E_k(\xi).$$

получаем равенство (10).

Для любого целого числа i, $i \in \{0, 2, 3, \dots\}$, имеем:

$$\xi^\tau E'_k(\xi) \nsubseteq M_i^{(1)},$$

откуда с учетом (16) получаем (15).

В обратную сторону. Пусть для множества M, $M \subseteq E'_k(\xi)$, выполнены (10) и (15) для $i = 0, 2, 3, \ldots$

Тогда из леммы 4 и соотношения (13) для некоторого $\tilde{\mu}$, $\tilde{\mu} = \frac{\tilde{u}}{\tilde{v}}$, $\deg(\tilde{u}) \geqslant \deg(\tilde{v})$, и любого a, $a \in E_k$, имеем:

$$\{a\tilde{\mu},\ a\xi\tilde{\mu}\} \subset K^1(M).$$

Поэтому, используя рассуждения из доказательства леммы 9 работы [7], заключаем, что существуют такие целые неотрицательные числа s_1 и s_2, что для любых таких целых неотрицательных чисел i и j, что $i \geqslant s_1$, $j \geqslant s_2$, имеем

$$\xi^i \tilde{\mu}^j \in K^1(M).$$

Поэтому для любого a, $a \in E_k$, и любых таких целых неотрицательных чисел i и j, что $i \geqslant s_1$, $j \geqslant s_2 + 1$, получаем:

$$a\xi^i \tilde{\mu}^j \subseteq K^1(M).$$

Отсюда и из условий (15) с использованием рассуждений из доказательства той же леммы работы [7] заключаем, что M — предельное множество.

Лемма доказана.

Положим

$$M_1^{(1)} = \left\{\mu \mid \mu \in E'_k(\xi), \mu(\xi) - \mu(0) \in \xi^2 \cdot E'_k(\xi)\right\}.$$

Имеем разложение числа m в произведение простых чисел q_1, q_2, ..., q_s:

$$m = q_1^{r_1} \cdot q_2^{r_2} \ldots q_l^{r_l}, \tag{17}$$

$q_s \neq q_{s'}$ при $s \neq s'$.

Обозначим через k_s число p^{m/q_s}, $s = 1, 2, \ldots, l$. Для любого s, $s = 1, 2, \ldots, l$, в поле E_k существует единственное подполе E_{k_s}, содержащее k_s элементов [6].

Для каждого s, $s \in \{1, 2, \ldots, l\}$, следующим образом определим множество $P_s^{(1)}$:

$$P_s^{(1)} = \{\mu(\xi) \mid \mu \in E'_k(\xi),\ \mu(0) \in E_{k_s}\}.$$

Теорема 3. *Пусть* $M \subseteq E'_k(\xi)$. *Равенство*

$$K^1(M) = E'_k(\xi) \tag{18}$$

выполнено в точности тогда, когда имеет место условие (10), *для любого* i, $i = 0, 1, \ldots$, *условие* (15), *а также для любого* s, $s \in \{1, 2, \ldots, l\}$, *следующее условие*:

$$M \not\subseteq P_s^{(1)}. \tag{19}$$

Доказательство. Пусть имеет место (18).

Через a обозначим какой-либо примитивный элемент поля E_k. Из (18) для множества M_0, $M_0 = \{\xi,\ a\}$, имеет место включение $M_0 \subset K^1(M)$. Учитывая, что $E_p(M_0) = E_k(\xi)$, получаем (10).

Справедливость соотношений (15) вытекает из неравенств

$$M_i^{(1)} \neq E'_k(\xi),\ i = 0, 1, \ldots$$

Свойство (19) множества M следует из K^1-замкнутости множеств $P_s^{(1)}$ и неравенств $P_s^{(1)} \neq E'_k(\xi)$, $s = 1, 2, \ldots, l$.

В обратную сторону. Пусть для множества M, $M \subseteq E'_k(\xi)$, выполнены соотношения (10), (15) при $i = 0, 1, \ldots,$ (19) при $s = 1, 2, \ldots, l$.

Для числа m имеем разложение (17). Через μ_s обозначим элемент множества M, не содержащийся в $P_s^{(1)}$, $s = 1, 2, \ldots, l$. Порядок числа b_s, $b_s = \mu_s(0)$, равен $p^{c_s \cdot q_s^{r_s}} - 1$ для некоторого делителя c_s числа $\frac{m}{q_s^{r_s}}$. Положим $c'_s = \sum_{i=0}^{c_s-1} p^{iq_s^{r_s}}$ Порядок числа d_s, $d_s = b_s^{c'_s}$, равен $p^{q_s^{r_s}} - 1$.

Отсюда и из [6] следует, что для любого s', $s' \in \{1, 2, \ldots, l\} \setminus \{s\}$, выполнены соотношения $d_s \in E_{k_{s'}}$ и $d_s \notin E_{k_s}$.

Поэтому число a_0, $a_0 = d_1 \cdot d_2 \cdot \ldots \cdot d_l$, не содержится в E_{k_s} для любого s, $s = 1, 2, ..., l$, то есть является примитивным элементом поля E_k.

Из приведенных рассуждений следует, что для любого a, $a \in E_k$, используя операцию умножения, из элементов множества M можно получить такую дробь μ_a, что $\mu_a(0) = a$.

Далее, ввиду соотношения $M \not\subseteq M_1^{(1)}$, в M содержится такая дробь μ', что для некоторых b'_0, b'_1, μ'', $\quad b'_0 \in E_k$, $\quad b'_1 \in E_k \setminus \{0\}$, $\quad \mu'' \in E'_k(\xi)$ выполнено

$$\mu' = b'_0 + b'_1 \xi \left(1 + \xi \mu''\right).$$

Используя дробь μ', а также дроби μ_a, $a \in E_k$, индукцией по s, $s \geqslant 1$, нетрудно показать, что для любого многочлена u, $u \in E_k[\xi]$, $\deg u < s$, найдется такая дробь μ_u из $E'_k(\xi)$, что

$$u + \xi^s \mu_u \in K^1(M).$$

Из этого и из леммы 8 следует, что $E_k[\xi] \subset K^1(M)$, откуда вытекает равенство (18).

Теорема доказана.

3. Редукция

Лемма 9. *Пусть*

$$h = \sum_{i=1}^{n} \mu_i \sum_{j=1}^{p} x_{i,j} + \sum_{i=1}^{n} \mu_i \sum_{j=1}^{p} x'_{i,j} + \mu' x' + \mu_0 \tag{20}$$

и

$$M = \{\mu_i \mid i = 1, 2, \ldots, n\}. \tag{21}$$

Тогда для любой μ, $\mu \in S^1(M)$, найдутся такие μ'' и ν, что

$$\mu x_1 + \mu x_2 + \mu'' x + \nu \in S(\{h\}). \tag{22}$$

Доказательство. Пусть имеют место равенства (20) и (21). Для л.-а. функции h справедливо равенство

$$\begin{aligned} h \;\; = \;\; & h\left(x_{1,1}, x_{1,2}, \ldots x_{1,p}, x_{2,1}, x_{2,2}, \ldots x_{2,p}, \ldots, x_{n,1}, x_{n,2}, \ldots x_{n,p},\right. \\ & \left. x'_{1,1}, x'_{1,2}, \ldots x'_{1,p}, x'_{2,1}, x'_{2,2}, \ldots x'_{2,p}, \ldots, x'_{n,1}, x'_{n,2}, \ldots x'_{n,p}\ , x'\right). \end{aligned}$$

Если $\mu \in S^1(M)$, то μ является многочленом от n переменных μ_1, μ_2, ..., μ_n степени, не меньшей 1.

Доказательство леммы проведем индукцией по степени $\deg_M(\mu)$ этого многочлена.

Если $\deg_M \mu = 1$, то найдутся такие числа $d_1, d_2, \ldots, d_n$ из E_p, что

$$\mu = \sum_{i=1}^{n} d_i \mu_i.$$

Положим

$$\begin{aligned} h'(x_1, x_2, x) \quad = \quad h \Bigg(& \underbrace{x_1, \ldots x_1}_{d_1}, \underbrace{x, \ldots, x}_{p-d_1}, \ldots, \underbrace{x_1, \ldots x_1}_{d_n}, \underbrace{x, \ldots, x}_{p-d_n}, \\ & \underbrace{x_2, \ldots x_2}_{d_1}, \underbrace{x, \ldots, x}_{p-d_1}, \ldots, \underbrace{x_2, \ldots x_2}_{d_n}, \underbrace{x, \ldots, x}_{p-d_n}, x \Bigg). \end{aligned}$$

Тогда для некоторых μ'' и ν выполнено (22).

Предположим, что для некоторого натурального числа r и любого μ, $\mu \in S^1(M)$, $\deg_M \mu \leqslant r$, найдутся такие μ'' и ν, что выполнено (22). Пусть μ, $\mu \in S^1(M)$, таково, что $\deg_M \mu = r + 1$.

Тогда найдутся такие числа d_j, $d_j \in E_p$, $j = 1, 2, \ldots, n$, и одноместные сохраняющие нулевую последовательность л.-а. функции μ'_j, $j = 1, 2, \ldots, n$, что $\mu'_j \in S^1(M)$, $\deg_M \mu'_j \leqslant r$, $j = 1, 2, \ldots, n$, и

$$\mu = \sum_{j=1}^{n} d_j \mu_j + \sum_{j=1}^{n} \mu_j \mu'_j.$$

Согласно предположению индукции, в $S(M)$ содержатся л.-а. функции $\tilde{h}_j(x, x_1)$,

$$\tilde{h}_j(x, x_1) = \mu'_j x + \mu'_j x_1 + \mu''_j x_1 + \nu_j.$$

Пусть

$$h'_j(x', x) \quad = \quad \begin{cases} \tilde{h}_j(x', x), & \text{если} \quad \tilde{h}_j(x', x) \neq 0, \\ x, & \text{если} \quad \tilde{h}_j(x', x) = 0, \end{cases}$$

$$\begin{aligned} \tilde{h}(x_1, x_2, x) \quad = \quad h \Bigg(& \underbrace{x_1, \ldots x_1}_{d_1}, h'_1(x_1, x), \underbrace{x, \ldots, x}_{p-d_1-1}, \ldots, \\ & \underbrace{x_1, \ldots x_1}_{d_n}, h'_n(x_1, x), \underbrace{x, \ldots, x}_{p-d_n-1}, \\ & \underbrace{x_2, \ldots x_2}_{d_1}, h'_1(x_2, x), \underbrace{x, \ldots, x}_{p-d_1-1}, \ldots, \\ & \underbrace{x_2, \ldots x_2}_{d_n}, h'_n(x_2, x), \underbrace{x, \ldots, x}_{p-d_n-1}, x \Bigg). \end{aligned}$$

Тогда для некоторых μ'' и ν выполнено (22). Лемма доказана.

В дальнейшем используем следующие множества одноместных л.-а. функций, сохраняющих нулевую последовательность:

$$W_i^{(1)} = \Big\{\mu \mid \mu \in M_i^{(1)}, \text{для некоторого}\, b, b \neq 0, \Psi_i(\mu) = (0, b)\Big\},$$

$$i = 0, 2, 3, \dots .$$

Лемма 10. *Для любого* μ, $\mu \in E'_k(\xi)$, *любого целого неотрицательного* τ *и любого* i, $i \in \{0, 2, 3, \dots\}$, *справедливы соотношения*

$$\mu \in M_i^{(1)} \Leftrightarrow \mu^{p^\tau} \in M_i^{(1)},$$

$$\mu \in W_i^{(1)} \Leftrightarrow \mu^{p^\tau} \in W_i^{(1)}.$$

Теорема 4. *Пусть для множества* M, $M \subseteq \mathfrak{L}_k$, *и любого* Θ, $\Theta \in J'_k$, *выполнено* (3). *Равенство* (4) *справедливо тогда и только тогда, когда* M *обладает следующими свойствами*:

$$E_p(U(M)) = E_k(\xi); \tag{23}$$

$$\forall s, s = 1, 2, \dots, l, \quad U(M) \nsubseteq P_s^{(1)}; \tag{24}$$

$$\forall j, j = 0, 1, 2, \dots, \quad U(K(M)) \nsubseteq M_j^{(1)}. \tag{25}$$

Доказательство. Пусть для множества M, $M \subseteq \mathfrak{L}_k$, выполнено (4). Тогда из (8) получаем равенство $K^1(U(M)) = E'_k(\xi)$. Поэтому $E_k \cup \{\xi\} \subset K^1(U(M))$. Отсюда и из включения $K^1(U(M)) \subseteq E_p(U(M))$ получаем (23). Свойство (24) вытекает из K^1-замкнутости собственных подмножеств $P_s^{(1)}$, $s = 1, 2, \dots, l$, множества $\mathfrak{L}_k$, свойство (25) — из неравенств $M_j^{(1)} \neq E'_k(\xi)$, $i = 0, 1, 2, \dots$

В обратную сторону. Пусть для M, $M \subseteq \mathfrak{L}_k$, выполнены (3), (23), (24) и (25). Докажем, что выполнено (5).

Из функции $f(x_1, x_2, \dots, x_n)$, $f \in M \setminus V_1$, с испольованием операций суперпозиции можно получить л.-а. функцию $g(x_1, x_2, x)$,

$$g(x_1, x_2, x) = \mu_1 \cdot x_1 + \mu_1 \cdot x_2 + \mu' \cdot x + \mu_0,$$

где $\mu_1(0) = 1$. Если $\mu_1 = 1$, то

$$x_1 + x_2 + \ldots + x_{p+1} = g(x_1, g(x_2, \dots g(x_p, x_{p+1}, x) \dots, x), x).$$

В противном случае одноместная л.-а. функция μ, $\mu = \mu_1^2 - \mu_1$, не содержится лишь в конечном множестве Ω классов системы $\{W_i^{(1)} \mid i = 0, 2, 3, \dots\}$. Положим

$$\Omega' = \{j \mid j \in \Omega, \ \mu \in M_j^{(1)}\} \cup \{1\}.$$

Согласно предположению, найдутся такие конечные множества M'_l, $l = 1, 2, 3$, что

$$M'_1 \subseteq U(M), \quad E_p(M'_1) = E_k(\xi),$$

$$M'_2 \subseteq U(M), \quad \forall s, s = 1, 2, \dots, l, \ M'_2 \nsubseteq P_s^{(1)},$$

$$M'_3 \subset K(U(M)), \quad \forall j, j \in \Omega', \ M'_3 \nsubseteq M_j^{(1)}.$$

Через r обозначим число $1 + \sum_{i=1}^{3} |M'_i|$. Выберем натуральное число τ, так, что $p^{\tau-1} \geqslant 2r$.

Положим

$$M_1'' = \{\mu_1^{p^\tau}\} \cup \{\ \mu' \mu_1^{p^\tau} \ \mid \ \mu' \in M_1'\},$$

$$M_2'' = \{\mu' \mu_1^{p^\tau} \ \mid \ \mu' \in M_2'\}.$$

Нетрудно видеть, что

$$E_p(M_1'') = E_k(\xi)$$

и

$$\forall s, s = 1, 2, \ldots, l, \quad M_2'' \not\subseteq P_s^{(1)}.$$

Для каждого $\mu' \in M_3'$ найдется такое натуральное число $T(\mu')$, что множество

$$M_3'' = \{(\mu')^{T(\mu')} \mu_1^{p^\tau} \ \mid \ \mu' \in M_3'\}$$

не содержится ни в одном из классов $M_j^{(1)}$, $j \in \Omega'$.

Пусть

$$M' = \bigcup_{l=1}^{3} M_l''.$$

Из свойств множества M', леммы 10 и теоремы 3 следует, что $1 \in K(M')$. Поэтому из леммы 5 вытекает, что для некоторых μ_i^*, $\mu_i^* \in S(M')$, $i = 1, 2$, имеет место равенство $1 = \frac{\mu_1^*}{1-\mu_2^*}$, откуда $1 = \mu_1^* + \mu_2^*$, то есть

$$1 \in S^1(M'). \tag{26}$$

Пусть

$$M' = \{\mu_j' \ \mid \ j = 1, 2, 3, \ldots, r\}.$$

Нетрудно видеть, что л.-а. функция h,

$$h = \sum_{i=1}^{r} \mu_i' \sum_{j=1}^{p} x_{i,j} + \sum_{i=1}^{r} \mu_i' \sum_{j=1}^{p} x_{i,j}' + \mu'' x + \mu_0'',$$

содержится в $K(M)$.

С учетом (26) из леммы 9 следует, что для некоторых μ^* и μ_0^* из $E_k'(\xi)$

$$x_1 + x_2 + \mu^* x + \mu_0^* \in S(\{h\}),$$

откуда, как было показано выше, следует (5).

Равенство (4) несложно получить, используя включение (5) и теорему 3.

Теорема доказана.

Переменная x_i л.-а. функции $f(x_1, x_2, \ldots, x_n)$, задаваемой равенством (1), называется существенной, если $\mu_i \neq 0$. Если $\mu_i(0) \neq 0$, то переменная x_i называется непосредственной.

Введем некоторые классы л.-а. функций:

$$\tilde{M}_0^{(1)} = \left\{\mu \ \mid \ \mu \in E_k'(\xi), \ \ \mu = \frac{u}{v}, \ \ \deg u < \deg v\right\},$$

$$\tilde{M}_i^{(1)} = \left\{\mu \ \mid \ \mu \in E_k'(\xi), \ \ \mu = \frac{u}{v}, \ \ (u, v) = 1, \ \ p_i \ \text{делит} \ u\right\}, i = 2, 3, \ldots,$$

$$R_i^{\text{С}} \;=\; \Big\{\, f \mid f \in \mathfrak{L}_k,\ \text{выполнено (1)}, \forall j, j=1,2,\dots,n,\ \text{если } x_j \text{ — единственная существенная переменная функции } f,\ \text{то } \mu_j \in M_i^{(1)},\ \text{в противном случае: } \mu_j \in \tilde{M}_i^{(1)} \Big\},$$

$$R_i^{\text{Н}} \;=\; \Big\{\, f \mid f \in \mathfrak{L}_k,\ \text{выполнено (1)}, \forall j, j=1,2,\dots,n,\ \text{если } x_j \text{ — единственная непосредственная переменная функции } f,\ \text{то } \mu_j \in M_i^{(1)},\ \text{в противном случае: } \mu_j \in \tilde{M}_i^{(1)} \Big\}, i = 0,2,3,\dots$$

Положим

$$J_k'' = \left\{ R_i^{\text{С}},\ R_i^{\text{Н}} \mid i = 0,2,3,\dots \right\}.$$

Следующее утверждение приведем без доказательства.

Теорема 5. *Каждый элемент множества J_k'' является K-замкнутым классом в $\mathfrak{L}_k$, не совпадающим с $\mathfrak{L}_k$.*

Обозначим через J_k следующее множество K-замкнутых классов:

$$J_k = J_k' \cup J_k''.$$

Лемма 11. *Пусть $i \in \{0,2,3,\dots\}$, $M \subseteq \mathfrak{L}_k$, $U(M) \subseteq M_i^{(1)}$,*

$$\forall\Theta, \Theta \in J_k' \cup \left\{R_i^C, R_i^н\right\},\ \text{имеет место } M \nsubseteq \Theta. \tag{27}$$

Соотношение

$$U(K(M)) \nsubseteq M_i^{(1)} \tag{28}$$

выполнено в точности тогда, когда

$$S^1(U(M)) \cap W_i^{(1)} \neq \varnothing. \tag{29}$$

Для доказательства этой леммы нам понадобится понятие i-сумматора. Л.-а. функция $g(x_1,x_2)$, $g(x_1,x_2) = \mu_1 x_1 + \mu_2 x_2 + \mu_0$, называется i-сумматором , $i \in \{0,2,3,\dots\}$, если $\mu_i(0) = 1$, $\mu_i - \mu_i(0) \in \tilde{M}_i^{(1)}$, $i = 1,2$.

Замечание 1. Если л.-а. функция f,

$$f(x_1,x_2,x) = \mu_1 x_1 + \mu_2 x_2 + \mu,$$

такова, что x_1 и x_2 — непосредственные переменные и $\mu_i \notin \tilde{M}_i^{(1)}$, $i = 1,2$, а $\nu \in E_k'$, то $S(\{f,\nu\})$ содержит i-сумматор.

Доказательство. Рассмотрим множество M л.-а. функций, не содержащееся для некоторого целого неотрицательного числа i, не равного 1, ни в одном из замкнутых классов множетва $J_k' \cup \{R_i^{\text{С}}, R_i^{\text{Н}}\}$, и такое, что $U(M) \subseteq M_i^{(1)}$.

Если имеет место (28), то из (8) с учетом лемм 6 и 7 заключаем, что неравенство (29) выполняется.

В обратную сторону: пусть имеет место (29), но (28) не выполнено. Сначала покажем, что в $K(M)$ содержится i-сумматор.

Рассмотрим функцию $g\,(x_1,x_2,\dots,x_m) \in M \setminus R_i^{\text{С}}$,

$$g\,(x_1,x_2,\dots,x_m) = \sum_{j=1}^{m} \mu_j' x_j + \mu'.$$

Без ограничения общности предположим, что $\mu_1' \notin \tilde{M}_i^{(1)}$ и $\mu_2' \neq 0$. По лемме 2 в $K(M)$ содержится некоторая константа ν. Тогда для л.-а. функции g',

$$g'(x_1, x_2) = g(x_1, x_2, \nu, \nu \ldots, \nu),$$

найдется такое μ_0', $\mu_0' \in E_k'(\xi)$, что

$$g'(x_1, x_2) = \mu_1' x_1 + \mu_2' x_2 + \mu_0'.$$

Случай 1. Если $\mu_1'(0) = 0$, то найдутся такие натуральные числа T и τ, что

$$\frac{\mu_2'}{1 - (\mu_1')^{T \cdot p^\tau}} \notin M_i^{(1)},$$

то есть выполнено (28), что противоречит предположению.

Случай 2. $\mu_1'(0) \neq 0$. Тогда рассмотрим следующие случаи.

Случай 2.1. $\mu_2' \notin \tilde{M}_i^{(1)}$. Тогда при $\mu_2'(0) = 0$, как и в случае 1, получим противоречие с предположением о не выполнимости соотношения (28), а при $\mu_2'(0) \neq 0$, учитывая последнее замечание, заключаем, что $K(M)$ содержит i-сумматор.

Случай 2.2. Пусть $\mu_2' \in \tilde{M}_i^{(1)}$. Рассматриваем:

Случай 2.2.1. $\mu_2'(0) \neq 0$. Тогда, используя операции суперпозиции, из функции $g'(x_1, x_2)$ и константы ν получим функцию $g''(x_1, x_2)$,

$$g'' = g'(\underbrace{g'(\ldots g'(g'}_{k-2 \text{ раз}}(x_1, \nu), \nu) \ldots,), \underbrace{g'(\nu, g'(\nu, \ldots g'}_{k-2 \text{ раз}}(\nu, x_2) \ldots))),$$

$$g''(x_1, x_2) = \mu_1'' x_1 + \mu_2'' x_2 + \mu_0'',$$

где $\mu_i'' = (\mu_i')^{k-1}$, $i = 1, 2$.

Имеем: $\mu_i''(0) = 1$, $i = 1, 2$, $\mu_1'' \notin \tilde{M}_i^{(1)}$, $\mu_2'' \in \tilde{M}_i^{(1)}$.

В $K(M)$ содержится л.-а. функция $\tilde{g}(x_1, x_2)$,

$$\tilde{g} = \underbrace{g''(x_1, g''(x_1, \ldots, g''}_{p \text{ раз}}(x_1, x_2) \ldots)),$$

Имеем

$$\tilde{g}(x_1, x_2, x_3) = \tilde{\mu}_1 x_1 + \tilde{\mu}_2 x_2 + \tilde{\mu}_0,$$

причем $\tilde{\mu}_1 = \sum_{j=0}^{p-1} \mu_1'' (\mu_2'')^j$, $\tilde{\mu}_2 = (\mu_2'')^p$, причем $\tilde{\mu}_1(0) = 0$, $\tilde{\mu}_1 \notin \tilde{M}_i^{(1)}$, $\tilde{\mu}_2 \neq 0$. Как показано в случае 1, используя л.-а. функцию $\tilde{g}$ и операции композиции, можно получить такую л.-.а. функцию $\hat{g}$, что $U(\hat{g}) \notin M_i^{(1)}$, что противоречит предположению.

Случай 2.2.2. $\mu_2'(0) = 0$. Тогда x_1 — единственная непосредственная переменная л.-а. функции

$$g' = g'(x_1, x_2).$$

По условию найдется л.-а. функция f, $f \in M \setminus R_i^{\text{н}}$, для которой выполнено (1).

Пусть x_1 не является единственной непосредственной переменной л.-а. функции f и $\mu_1 \notin \tilde{M}_i^{(1)}$.

Если $\mu_1(0) = 0$, то из функции

$$g'(f(x_1, \nu, \nu, \ldots, \nu), x_2),$$

как и в случае 1, с использованием операций композиции можно получить такую л.-а. функцию $\tilde{f}$, что $U(\tilde{f}) \notin M_i^{(1)}$, то есть выполнено (28), что противоречит предположению.

Если $\mu_1(0) \neq 0$, то среди переменных $x_2, x_3, \ldots x_n$ л.-а. функции f есть непосредственная переменная. Предположим, что x_2 — непосредственная переменная функции f. Тогда для л.-а. функции $f(x_1, x_2, \nu, \nu, \ldots, \nu)$ можно применить либо рассуждения случая 2.1, если $\mu_2 \notin \tilde{M}_i^{(1)}$, либо рассуждения случая 2.2.1, если $\mu_2 \in \tilde{M}_i^{(1)}$.

Таким образом, $K(M)$ содержит i-сумматор $h(x_1, x_2)$,

$$h = \nu_1 x_1 + \nu_2 x_2 + \nu_0.$$

Пусть $f_j \in \mathfrak{L}_k$,

$$f_j\left(x_{j,1}, x_{j,2}, \ldots, x_{j,n_j}\right) = \sum_{r=1}^{n_j} \mu_{j,r} x_{j,r} + \mu_{j,0},$$

$j = 1, 2$. Выберем произвольно r_j, $r_j \in \{1, 2, \ldots, n_j\}$, $j = 1, 2$. Тогда, как нетрудно видеть,

$$\begin{aligned}\Psi_i(\mu_{1,r_1} \cdot \mu_{2,r_2}) \quad \in \quad & \Psi_i\left(U\left(f_1\left(x_{1,1}, x_{1,2}, \ldots, x_{1,r_1-1},\right.\right.\right.\\ & \left.\left.\left. f_2\left(x_{2,1}, x_{2,2}, \ldots, x_{2,n_2}\right), x_{1,r_1+1}, \ldots, x_{1,n_1}\right)\right)\right),\end{aligned}$$

$$\begin{aligned}\Psi_i(\mu_{1,r_1} + \mu_{2,r_2}) \quad \in \quad & \Psi_i\left(U\left(h\left(f_1(x_{1,1}, x_{1,2}, \ldots, x_{1,r_1}, \ldots, x_{1,n_1})\right.\right.\right.\\ & \left.\left.\left. f_2(x_{2,1}, x_{2,2}, x_{2,r_2}, \ldots, x_{2,n_2})\right)\right)\right),\end{aligned}$$

Отсюда и из соотношения (29) следует, что в $S(M)$ найдется такая л.-а. функция f_3,

$$f_3 = \sum_{j=1}^{n_3} \mu_{3,j} x_{3,j} + \mu_{3,0},$$

что для некоторого j_0, $j_0 \in \{1, 2, \ldots, n_3\}$, и для некоторого b, $b \neq 0$,

$$\Psi_i\left(\mu_{3,j_0}\right) = (0, b).$$

Положим

$$f_4(x) = f_3\left(\underbrace{\nu, \nu, \ldots, \nu}_{j_0-1 \text{ раз } \nu}, x, \nu, \nu, \ldots, \nu\right).$$

Тогда $U(f_4) = \{\mu_{3,j_0}\}$.

Пусть $T \in \mathbb{N}$. Применив операцию обратной связи к переменной x_2 л.-а. функции $h\left(x_1, f_4^T(x_2)\right)$, получим л.-а. функцию $f_{5,T}(x_1)$, для которой $U(f_{5,T}) = \left\{\text{Об}\left(\nu_1, \mu_{3,j_0}^T\right)\right\}$.

Найдется такое T_0, что Об $\left(\nu_1, \mu_{3,j_0}^{T_0}\right) \not\subseteq M_i^{(1)}$. Получили противоречие с предположением, что (28) не выполнено. Лемма доказана.

Теорема 6. *Проблема проверки K-полноты конечных множеств из $\mathfrak{L}_k$ алгоритмически разрешима.*

Доказательство. Рассмотрим конечное множество M л.-а. функций. Сначала проверим соотношение (3) для каждого Θ, $\Theta \in J'_k$. Если хотя бы одно из этих соотношений не выполнено, то по теореме 1 множество M не является K-полным.

В противном случае проверяем соотношение (23). Для этого выбираем какое-либо η, $\eta \in U(M) \setminus E_k$ (если такого η не существует, то M не является K-полным) и проверяем равенство (11). Если оно не выполнено, то, согласно следствию из леммы 3, включению $U(K(M)) \subseteq E_p(M)$ и теореме 4, множество M не является K-полным. Если равенство (11) имеет место, то проверяем справедливость включений $M \subseteq P_s^{(1)}$, $s = 1, 2, \dots, l$. Выполнение хотя бы одного из них по теореме 4 означает, что M не является K-полным.

Если ни одно из рассматриваемых включений не выполнено, то по теореме 4 остается проверить свойство (25).

Нетрудно видеть, что включения $U(K(M)) \subseteq M_1^{(1)}$ и $U(M) \subseteq M_1^{(1)}$ равносильны, причем второе из них несложно проверить.

Далее следующим образом убеждаемся в справедливости соотношений

$$U(K(M)) \nsubseteq M_i^{(1)} \tag{30}$$

для любого i, $i \in \{0, 2, 3, \dots\}$. Для данного i соотношение (30) следует из того, что $U(M) \nsubseteq M_i^{(1)}$.

Положим

$$I = \left\{ i \mid U(M) \subseteq M_i^{(1)} \right\}.$$

При $i \in I$ по лемме 11 соотношение (30) выполнено, если имеют место (29) и (27). Рассмотрим л.-а. функцию f, $f \in M \setminus V_1$. Пусть справедливо разложение (1) и, без ограничения общности, x_1, x_2 — непосредственные переменные функции f.

Пусть $\mu_1 = \frac{u_1}{v_1}$. Если неприводимый многочлен p_j, $j \in \{2, 3, \dots\}$, не делит u_1, то $f \notin R_j^{\text{С}}$ и $f \notin R_j^{\text{Н}}$. Поэтому можно проверить, верно ли свойство:

$$\forall i, i \in \{0, 2, 3, \dots\}, \left(M \nsubseteq R_i^{\text{С}} \wedge M \nsubseteq R_i^{\text{Н}} \right).$$

Если это свойство не выполнено, то по теореме 4 множество M не является K-полным.

В противном случае множество

$$\left\{ j \mid \eta - \eta^k \notin W_j^{(1)} \right\}$$

конечно. Поэтому свойство ($\forall j \in I$ выполнено (29)) может быть проверено. Теорема доказана.

Список литературы

1. Ван дер Варден Б. Л., *Алгебра*, пер. с нем., Наука, Москва, 1976, 648 с.
2. Гилл А., *Линейные последовательностные машины*, пер. с англ., Наука, Москва, 1974, 288 с.
3. Зарисский О., Самюэль П., *Коммутативная алгебра*, пер. с англ., ИЛ, Москва, 1963, 373 с.
4. Кудрявцев В. Б., Алешин С. В., Подколзин А. С., *Введение в теорию автоматов*, Наука, Москва, 1985, 320 с.

5. Ленг С., *Алгебра*, пер. с англ., Мир, Москва, 1968, 564 с.
6. Лидл Р., Нидеррайтер Г., *Конечные поля.*, пер. с англ., **1**, Мир, Москва, 1988, 430 с.
7. Часовских А. А., "Условия полноты линейно-р-автоматных функций", *Интеллектуальные системы*, **18**:3 (2014), 203–252.
8. Lau D., *Function Algebras on Finite Sets. A Basic Course on Many-Valued Logic and Clone Theory*, Springer, Rostok, 2006, 668 c.
9. Szendrei Á., "On closed classes of quasilinear functions", *Chechoslovak Math. J.*, **30**:3 (1980), 498–509.

Статья поступила 17.03.2015.