

Критериальные системы в классах линейно-автоматных функций над конечными полями

А. А. Часовских

Получены счетные критериальные системы замкнутых подклассов в классах линейно-автоматных функций над конечными полями.

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

В работе [6] решена задача о полноте в классах линейно-автоматных функций (л.-а. функций) над простыми конечными полями. В [7] найден алгоритм проверки полноты по операциям композиции конечных подмножеств в классах линейно-автоматных функций. Здесь мы будем использовать определения и обозначения из этих работ, продолжая изучение классов линейно-автоматных функций \mathcal{L}_k над конечными полями E_k , где $k = p^m$, p - простое число, а m - натуральное число. Через $R_k(\xi)$ обозначим множество всех формальных рядов переменной ξ с коэффициентами из E_k . Линейно-автоматной функцией мы называем отображение $f(x_1, x_2, \dots, x_n)$ из $R_k(\xi)^n$ в $R_k(\xi)$, которое реализуется линейной последовательностной машиной [2].

Через $E_k(\xi)$ обозначим поле отношений многочленов переменной ξ с коэффициентами из E_k . Подкольцо $E'_k(\xi)$ этого поля, состоящее из дробей, знаменатель которых в несократимом виде имеет свободный член отличный от нуля, обозначаем $E'_k(\xi)$.

Нетрудно видеть, что $E'_k(\xi)$ изоморфно подкольцу всех рядов из $R_k(\xi)$, коэффициенты которых образуют периодическую (с предпериодом) последовательность.

При этом для заданной л.-а. функции $f(x_1, x_2, \dots, x_n)$ найдутся такие дроби $\mu_i, \mu_i \in E'_k(\xi), i = 0, 1, \dots, n$, что выполнено:

$$f(x_1, x_2, \dots, x_n) = \sum_{i=1}^n \mu_i x_i + \mu_0. \quad (1)$$

Переменная x_i л.-а. функции f , заданной равенством (1), называется существенной, если $\mu_i \neq 0$, и называется непосредственной, если $\mu_i(0) \neq 0$.

Через V_1 обозначим множество всех л.-а. функций, имеющих не более одной непосредственной переменной.

Пусть для л.-а. функции f выполнено (1). Положим

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

Для множества $M, M \subseteq \mathfrak{L}_k$, определим

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

Через V_p обозначим множество всех л.-а. функций f таких, что

$$\sum_{\mu \in U(f)} \mu(0) = 1.$$

Показатель m разложим в произведение простых чисел q_1, q_2, \dots, q_l :

$$m = q_1^{r_1} \cdot q_2^{r_2} \cdot \dots \cdot q_l^{r_l},$$

$q_s \neq q_{s'}$ при $s \neq s'$. Пусть $s \in \{1, 2, \dots, l\}$ и $k_s = p^{m/q_s}$. Известно [5], что поле E_k , содержит единственное подполе из k_s элементов, которое мы будем обозначать E_{k_s} .

Множество всех л.-а. функций f таких, что для любого $\mu, \mu \in U(f)$, выполнено: $\mu(0) \in E_{k_s}$ обозначим P_s .

Каждой л.-а. функции f сопоставим квазилинейную функцию $\lambda(f)$, которая набору $(a_1, a_2, \dots, a_n), a_i \in E_k$, ставит в соответствие свободный член ряда $f(a_1, a_2, \dots, a_n)$

Критериальные системы в классах линейно-автоматных функций над конечными полями

Обозначим через T_a множество всех л.-а. функций f , что $\lambda(f)$ сохраняет элемент a поля E_k .

Далее, как уже отмечалось, будем использовать обозначения из работ [6] и [7].

Положим

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

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

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

$$M_1 = \left\{ f \mid f \in \mathfrak{L}_k, U(f) \subseteq M_1^{(1)} \right\}.$$

Упорядочим все неприводимые в $E_k[\xi]$ приведенные многочлены: $p_1(\xi), p_2(\xi), \dots$ так, что $p_1(\xi) = \xi$. Положим

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

$$\tilde{M}_i^{(1)} = \left\{ \mu \mid \mu \in E'_k(\xi), \mu = \frac{u}{v}, p_i \mid u \right\}, \quad i = 2, 3, \dots$$

В дальнейшем нам понадобятся следующие множества л.-а. функций

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

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

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

Для дроби $\mu = \frac{u}{v}$ из $M_0^{(1)}$ найдутся такие r, a_i, b_i, u_i , что $r \in \mathbb{N}$, $a_i, b_i \in E_k$, $u_i \in E_k[\xi]$, $i = 0, 1$, $a_1 \neq 0$, $b_1 \neq 0$, что выполнено равенство:

$$\mu = \frac{a_0 + \xi u_0 + b_0 \xi^r}{a_1 + \xi u_1 + b_1 \xi^r}.$$

Для такой дроби положим $\Psi_0(\mu) = \left(\frac{a_0}{a_1}, \frac{b_0}{b_1} \right)$.

Множеству M , $M \subseteq M_0^{(1)}$, соответствует конечное множество $\Psi_0(M)$ пар чисел из E_k :

$$\{ \Psi_0(\mu) \mid \mu \in M \},$$

замыкание которого по операциям покомпонентного сложения и умножения обозначим $S(\Psi_0(M))$.

Определим следующие множества.

$$M_{0,s}^{(1)} = \left\{ \mu \mid \mu \in M_0^{(1)}, \Psi_0(\mu) \in \{(c', c) \mid c' \in E_k, c \in P_{k_s}\} \right\},$$

$$M_{0,s} = \left\{ f \mid f \in \mathfrak{L}_k, U(f) \subset M_{0,s}^{(1)} \right\}.$$

Пусть a - примитивный элемент поля E_k , а b - сопряженный к нему относительно поля E_p [1]. Любому c , $c \in E_k \setminus \{0\}$, например, сопряженным относительно поля E_p является само c . Отображение $\omega : E_k \rightarrow E_k$ такое, что $\omega(0) = 0$ и $\omega(a^i) = b^i$, $i = 1, 2, \dots, k-1$, является автоморфизмом поля E_k . Поэтому для любого многочлена $\phi(x)$, $\phi(x) \in E_p[x]$, такого, что $\phi(a) = 0$, справедливо равенство: $\phi(b) = 0$. Положим

$$M_{0,\omega}^{(1)} = \left\{ \mu \mid \mu \in M_0^{(1)}, \Psi_0(\mu) \in \{(c, \omega(c)) \mid c \in E_k\} \right\},$$

$$M_{0,\omega} = \left\{ f \mid f \in \mathfrak{L}_k, U(f) \subset M_{0,\omega}^{(1)} \right\}.$$

Лемма 1. Пусть для некоторого M , $M \subseteq M_0^{(1)}$, для любого s выполнено:

$$M \not\subseteq M_{0,s}^{(1)}, \quad (2)$$

Критериальные системы в классах линейно-автоматных функций над конечными полями

а также для любого ω имеет место:

$$M \not\subseteq M_{0,\omega}^{(1)}. \quad (3)$$

Тогда для некоторой ненулевой константы c , $c \in E_k$, справедливо включение:

$$(0, c) \in \Psi_0(S^1(M)),$$

где через $S^1(M)$ обозначено замыкание множества M по операциям сложения и умножения.

Доказательство. Сначала заметим, что справедливо равенство:

$$\Psi_0(S^1(M)) = S(\Psi_0(M)).$$

Пусть для некоторого множества M , $M \subseteq M_0^{(1)}$, любого числа s , $s \in \{1, 2, \dots, l\}$, выполнено (2), а для любого автоморфизма ω поля E_k справедливо (3). Из соотношений (2) следует, что для любого c , $c \in E_k$ найдется c' , $c' \in E_k$ такое, что

$$(c', c) \in S(\Psi_0(M)).$$

При этом, если для различных чисел c_1 и c_2 найдется одно и то же c' такое, что $(c', c_1) \in S(\Psi_0(M))$ и $(c', c_2) \in S(\Psi_0(M))$, то $(0, c_1 - c_2) \in S(\Psi_0(M))$ и лемма доказана.

В противном случае, для некоторого примитивного элемента a поля E_k и некоторого c , $c \in E_k$, имеем: $(c, a) \in S(\Psi_0(M))$. Если c не является примитивным элементом поля E_k и не равен нулю, то его порядок r меньше $k - 1$. Поэтому из равенства $(c, a)^r - (c, a)^{k-1} = (0, a^r - 1)$ следует утверждение леммы.

Далее рассмотрим случай, когда в $S(\Psi_0(M))$ содержится пара (c, a) , состоящая из примитивных элементов поля E_k . Пусть при этом найдется еще c' , $c' \in E_k$, $c' \neq c$, такое, что $(c', a) \in S(\Psi_0(M))$. Тогда в кольце $E_p[z]$ найдется многочлен $u(z)$ степени ниже t , не совпадающий с z , такой, что в поле E_k выполнено равенство: $u(c) = c'$. Имеем: $(c' - u(c), a - u(a)) = (0, a - u(a)) \in S(\Psi_0(M))$. Выражение $a - u(a)$ является ненулевым многочленом из $E_p[a]$ степени не выше $t - 1$. Поэтому из примитивности элемента a в поле E_k следует, что элемент

$a - u(a)$ поля E_k не равен нулю. Поэтому утверждение леммы в рассматриваемом случае справедливо.

Пусть теперь для какого-то элемента $u(a)$ поля E_k , $u(a) \in E_p[a]$ имеется два различных элемента c'_i , $i = 1, 2$, такие что $(c'_i, u(a)) \in S(\Psi_0(M))$, $i = 1, 2$. Тогда $(c'_1 - c'_2, 0) \in S(\Psi_0(M))$. Поэтому $(c + c'_1 - c'_2, a)$ и доказательство сводится к ранее рассмотренному случаю.

Таким образом, осталось рассмотреть случай:

$$S(\Psi_0(M)) = \{ (u(c), u(a)) \mid u(a) \in E_p[a], \deg(u(a)) \leq m - 1 \}.$$

При этом, если элементы a и c поля E_k не являются сопряженными, то для некоторого $a' \in E_k \setminus \{0\}$ получаем $(0, a') \in S(\Psi_0(M))$ и утверждение леммы выполнено. Если же a и c являются сопряженными, то не выполнено (3).

Лемма доказана.

Рассмотрим отображения Ψ_i , $i = 2, 3, \dots$, которые соответствуют приведенным неприводимым в $E'_k[\xi]$ многочленам $p_i(\xi)$, $p_i(\xi) \neq \xi$. При этом каждой дроби μ из $E'_k(\xi)$, знаменатель которой не делится на $p_i(\xi)$, отображение Ψ_i сопоставляет пару $(\mu(0), u(\xi))$, в которой $u(\xi) \in E'_k[\xi]$, $\deg u(\xi) \leq \deg p_i(\xi)$ и для некоторой μ' , $\mu' \in E'_k(\xi)$, знаменатель которой тоже не делится на $p_i(\xi)$, имеет место равенство:

$$\mu(\xi) = u(\xi) + \xi p_i(\xi) \mu'(\xi). \quad (4)$$

Рассмотрим некоторое изоморфное вложение γ поля E_k в кольцо многочленов из $E'_k[\xi]$, рассматриваемых по модулю многочлена $\xi p_i(\xi)$, такое, что для любого a , $a \in E_k$, выполнено: $\gamma_i(a)(0) = a$. Примерами таких вложений могут быть отображения $\gamma_{i,1}(a) = a$ и $\gamma_{i,2}(a) = a p(\xi)$. Множество всех таких вложений обозначим Γ_i .

Для заданного вложения γ , $\gamma \in \Gamma_i$, положим:

$$M_{i,\gamma}^{(1)} = \left\{ \mu(\xi) \mid \mu \in M_i^{(1)}, \Psi_i(\mu(0)) \in \{ (a, \gamma(a)) \mid a \in E_k \} \right\}.$$

В дальнейшем также используются множества:

$$M_{i,\gamma} = \left\{ f \mid f \in \mathfrak{L}_k, U(f) \subset M_{i,\gamma}^{(1)} \right\}.$$

Лемма 2 Пусть для некоторого i , $i \in \{2, 3, \dots\}$, имеет место: $M \subseteq M_i^{(1)}$, для любого s , $s = 1, 2, \dots, l$, выполнено:

$$M \not\subseteq P_s^{(1)}, \quad (5)$$

а также для любого вложения γ , $\gamma \in \Gamma_i$, справедливо:

$$M \not\subseteq M_{i,\gamma}^{(1)}. \quad (6)$$

Тогда для некоторого ненулевого многочлена u , $u \in E_k[\xi]$, $\deg(u) \leq \deg(p_i)$, справедливо включение:

$$(0, u) \in \Psi_i(S^1(M)).$$

Доказательство. Рассмотрим множество M , $M \subseteq M_i^{(1)}$, удовлетворяющее для любого s , $s = 1, 2, \dots, l$, условию (5).

Тогда для любого μ , $\mu \in M$, определена пара $\Psi_i(\mu)$, $\Psi_i(\mu) = (\mu(0), u(\xi))$, где $u(\xi) \in E_k[\xi]$, $\deg u(\xi) \leq \deg p_i(\xi)$ и для некоторого $\mu'(\xi)$, $\mu'(\xi) \in M_i^{(1)}$ выполнено: (4).

Из справедливости (5) для любого s , $s = 1, 2, \dots, l$, следует, что множество $R = \{ u(\xi) \mid \Psi_i(\mu) = (\mu(0), u(\xi)), \mu \in S^1(M) \}$ содержит не менее k элементов. Если для некоторого a , $a \in E_k$, найдутся два различных многочлена $u_i(\xi)$, $i = 1, 2$, таких, что $(a, u_i(\xi)) \in \Psi(M)$, то $(0, u_1(\xi) - u_2(\xi)) \in \Psi_i(S^1(M))$. Поэтому остается рассмотреть случай $|R| = k$.

В этом случае рассмотрим отображение γ , $\gamma : E_k \rightarrow E_k[\xi]$, сопоставив каждому элементу a поля E_k вторую компоненту пары $(\mu(0), u(\xi))$, где $\mu(0) = a$. Нетрудно видеть, что отображение γ является изоморфным вложением поля E_k .

Поэтому (6) не выполнено. Лемма доказана.

Подполе K поля $E_k(\xi)$ называется его максимальным подполем если оно не совпадает с $E_k(\xi)$ и не содержится ни в одном другом подполе, которое не совпадает с $E_k(\xi)$.

Примером максимального подполя в $E_k(\xi)$ может служить поле $E_k(\xi^2)$, являющееся расширением [1] поля E_k многочленным ξ^2 . Действительно, $E_k(\xi)$ является линейным пространством размерности 2 над полем $E_k(\xi^2)$. Базисом этого линейного пространства является множество $\{1, \xi\}$. Пусть $\eta \in E_k(\xi) \setminus E_k(\xi^2)$.

Тогда найдутся $\mu_i, \mu_i \in E_k(\xi^2), i = 1, 2$, такие, что $\eta = \mu_1 + \xi \cdot \mu_2$ и $\mu_2 \neq 0$. Тогда $\xi = (\eta - \mu_1)/\mu_2$ и поле, содержащее $E_k(\xi^2)$ и η совпадает с $E_k(\xi)$. Таким образом, доказано, что $E_k(\xi^2)$ - максимальное подполе в $E_k(\xi)$.

Далее нам понадобится множество $\{ B_q \mid q \in Q \}$, состоящее из всех максимальных подполей поля $E_k(\xi)$.

Положим

$$J_k = \{ V_1, V_p, P_s, T_a, M_{0,s}, M_{0,\omega}, M_1, M_{i,\gamma}, R_i^C, R_i^H, B_q \mid \\ s \in \{1, 2, \dots, l\}, a \in E_k, \omega \in \Omega, i \in \{2, 3, \dots\}, \gamma \in \Gamma_i, q \in Q \}.$$

Для множества M л.-а. функций положим $\lambda(M) = \{ \lambda(f) \mid f \in M \}$. Множество всех квазилинейных функций над полем E_k , как и в работе [9] будем обозначать L_k . Замыкание множества $M, M \subseteq L_k$, по операциям суперпозиции обозначим $S(M)$.

Далее приведем доказательство результата, полученного в [8].

Лемма 3. Если $M \subseteq \mathfrak{L}_k$ и $M \not\subseteq \Theta$ для любого $\Theta, \Theta \in J'_k$,

$$J'_k = \{ V_1, V_p, P_s, T_a \mid s \in \{1, 2, \dots, l\}, a \in E_k \},$$

то выполнено равенство

$$S(\lambda(M)) = L_k. \tag{7}$$

Доказательство. Пусть для $M, M \subseteq \mathfrak{L}_k$, и любого $\Theta, \Theta \in J'_k$, выполнено: $M \not\subseteq \Theta$.

Тогда найдется функция $f(x_1, x_2, \dots, x_n)$,

$$f(x_1, x_2, \dots, x_n) \in M \setminus V_1.$$

Не ограничивая общности рассуждений, будем предполагать, что x_1 и x_2 - непосредственные переменные функции f . Через $f'(x_1, x_2, x)$ обозначим квазилинейную функцию $\lambda(f(x_1, x_2, x \dots, x))$.

Для квазилинейной функции $f''(x_1, x_2, x)$,

$$f''(x_1, x_2, x) = f'(f'(x, x_1, x), f'(x_2, x, x), x),$$

Критериальные системы в классах линейно-автоматных функций над конечными полями

в E_k найдутся такие c, c_0, c_1 , что $c \neq 0$ и

$$f''(x_1, x_2, x) = c \cdot x_1 + c \cdot x_2 + c_1 \cdot x + c_0.$$

В поле E_k имеет место равенство $c^{k-1} = 1$. Поэтому для квазилинейной функции $\tilde{f}(x_1, x_2, x)$,

$$\tilde{f} = \underbrace{f''(f''(\dots f''(f''(x_1, x_2, x), x, x) \dots, x, x), x, x)}_{k-1 \text{ раз } f''},$$

в E_k найдутся такие c'_0 и c'_1 , что выполнено равенство

$$\tilde{f}(x_1, x_2, x) = x_1 + x_2 + c'_1 x + c'_0.$$

Тогда получим квазилинейный сумматор от $p+1$ переменных

$$x_1 + x_2 + \dots + x_{p+1} = \underbrace{\tilde{f}\left(\tilde{f}\left(\dots \tilde{f}\left(\tilde{f}(x_1, x_2, x), x_3, x) \dots, x_p, x\right), x_{p+1}, x\right)}_p \text{ раз } \tilde{f}.$$

Из квазилинейной функции $\lambda(g)$, $g \in M \setminus V_p$, используя операции отождествления и переименования переменных, получаем функцию $g'(x)$, $g'(x) = d \cdot x + d'$, причем $d \in E_k \setminus \{1\}$, $d' \in E_k$.

Если $g'(x)$ не является константой, то $d \neq 0$ и найдется такое натуральное число r , что $d^r = d + 1$. Тогда для некоторого d'' имеем

$$(g')^r(x) = (d + 1) \cdot x + d''.$$

Поэтому квазилинейная функция

$$x + g'(x) + \underbrace{(g')^r(x) + \dots + (g')^r(x)}_{p-1 \text{ слагаемых}}$$

является константой.

Таким образом, в $S(\lambda(M))$ содержится некоторая константа $\tilde{d}, \tilde{d} \in E_k$.

Докажем, что в $S(\lambda(M))$ содержится нулевая константа. Пусть $\tilde{d} \neq 0$. Из соотношения $M \not\subseteq T_{\tilde{d}}$ следует, что, подставляя константу \tilde{d} в некоторую функцию из $\lambda(M)$, получим константу \hat{d} , $\hat{d} \neq \tilde{d}$.

Через a обозначим элемент поля E_k , равный $\frac{\tilde{d}}{\hat{d}-\tilde{d}}$.

Используя соотношения $M \not\subseteq P_s$, $s = 1, 2, \dots, l$, нетрудно показать, что для любого a' , $a' \in E_k$, найдется a'' , $a'' \in E_k$, что выполнено соотношение: $a' \cdot x + a'' \in S(\lambda(M))$. Используя функцию f_a , $f_a = a \cdot x + a''$, а также сумматор $x_1 + x_2 + \dots + x_{p+1}$ и операции суперпозиции, получаем квазилинейную функцию \tilde{f}_a , $\tilde{f}_a = a \cdot x_1 + a \cdot x_2 + \dots + a \cdot x_p + x$. Нетрудно видеть, что функция $\tilde{f}_a(\hat{d}, \dots, \hat{d}, \tilde{d}, \tilde{d})$ совпадает с нулевой константой.

Пусть теперь $h(x_1, x_2, \dots, x_n)$ - какая-либо квазилинейная функция,

$$h(x_1, x_2, \dots, x_n) = \sum_{i=1}^n a_i \cdot x_i + a_0.$$

Из сумматора $x_1 + x_2 + \dots + x_{p+1}$ и нулевой константы с использованием операций суперпозиции нетрудно получить $n + 1$ -местный сумматор.

Пусть $a' \in E_k$. Как отмечалось, в $S(\lambda(M))$ содержится квазилинейная функция $\tilde{f}_{a'}$, $\tilde{f}_{a'} = a' \cdot x_1 + a' \cdot x_2 + \dots + a' \cdot x_p + x$. Подстановкой нуля и переименованием переменных из функции $\tilde{f}_{a'}$ получаем множитель $a' \cdot x$. Далее, среди констант \tilde{d} и \hat{d} есть ненулевая, которую мы обозначим d_0 . Тогда квазилинейная функция $\frac{a_0}{d_0} \cdot d_0$ реализует константу a_0 и содержится в $S(\lambda(M))$.

Функцию $h(x_1, x_2, \dots, x_n)$ получаем подстановкой множителей $a_i \cdot x_i$, $i = 1, 2, \dots, n$, и константы a_0 вместо соответствующих переменных сумматора $x_1 + x_2 + \dots + x_n + x$

Лемма доказана.

Теорема. Множество J_k является счетной критериальной системой замкнутых классов [4] в \mathfrak{L}_k .

Доказательство. Замкнутость классов, содержащихся в J_k , и их несовпадение с \mathfrak{L}_k доказывается путем проверки.

Критериальные системы в классах линейно-автоматных функций над конечными полями

Пусть $M \subseteq \mathfrak{L}_k$ и для любого Θ , $\Theta \in J_k$, выполнено: $M \not\subseteq \Theta$. Из рассуждений, приведенных в [7], и леммы 3 можно заключить, что для полноты множества M достаточно выполнения следующих трех условий.

1. M не содержится ни в одном из замкнутых классов системы

$$\{ V_1, V_p, P_s, T_a, M_1, R_i^C, R_i^H \mid s \in \{1, 2, \dots, l\}, a \in E_k, i \in \{2, 3, \dots\} \}.$$

2. Для каждого i , $i = 0, 2, 3, \dots$, из включения $U(M) \subseteq M_i^{(1)}$ следует, что найдется ненулевое c , для которого выполнено: $(0, c) \in \Psi_i(S^1(M))$.

3. $E_p(M) = E_k(\xi)$.

Из лемм 1 и 2 следует, что условие 2 выполнено, если M не содержится ни в одном из замкнутых классов множества

$$\{M_{0,s}, M_{0,\omega}, P_s, M_{i,\gamma} \mid s \in \{1, 2, \dots, l\}, \omega \in \Omega, i \in \{2, 3, \dots\}, \gamma \in \Gamma_i\}.$$

Из [3] следует, что для любого элемента η поля $E_k(\xi)$ ненулевой степени поле $E_k(\xi)$ является линейным пространством конечной размерности над полем $E_p(\eta)$, получаемым расширением простого поля E_p элементом η . Отсюда и из рассмотренного выше примера поля $E_k(\xi^2)$ следует, что любое собственное подполе в $E_k(\xi)$ содержится в некотором его максимальном подполе, число которых не более чем счетно. Таким образом, условие 3 вытекает из невключения M ни в один из классов множества

$$\{B_q \mid q \in Q\}.$$

Теорема доказана.

Список литературы

- [1] Ван дер Варден Б. Л. Алгебра. – Наука. Москва, 1976, 648 с.
- [2] Гилл А. Линейные последовательностные машины. – Наука. Москва, 1974, 288 с.

- [3] Зарисский О., Самюэль П. Коммутативная алгебра. – 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] Лидл Р., Нидеррайтер Г. Конечные поля. – Мир. Москва, 1988, 430 с.
- [6] Часовских А. А. Условия полноты линейно-р-автоматных функций // Интеллектуальные системы. – 2014. Т. 18, вып. 3. – С. 203 -252.
- [7] Часовских А. А., Проблема полноты для класса линейно-автоматных функций // Дискретная математика. – 2015. Т. 27, вып. 2. – С. 134 - 151.
- [8] Часовских А. А., Проблема А-полноты линейно-автоматных функций // Интеллектуальные системы. – 2014. Т. 18, вып. 1. – С. 253 - 257.
- [9] Szendrei Á. On closed classes of quasilinear functions // Chechoslovak Math. J. – 1980. Т. 30, вып. 3. – С. 498 - 509.

Criteria systems in classes of linear automaton functions over finite fields

A. A. Chasovskikh

Countable criteria systems of closed subclasses in classes of linear automaton functions over finite fields received.

Keywords: finite automata, function of linear automaton, operation of composition, operation of superposition, feedback, completeness problem, closed subclass, criteria system, adder, delay.