Приведенные критериальные системы предполных классов в классах линейных автоматов над конечными полями

Часовских А.А.

Найдены множества всех предполных классов в классах линейных автоматов над конечными полями, являющиеся приведенными критериальными системами в этих классах.

Ключевые слова: конечный автомат, линейный автомат, операции композиции, операции суперпозиции, обратная связь, проблема полноты, предполный класс, критериальная система, приведенная критериальная система, сумматор, задержка.

Мы будем использовать понятия и обозначения, введенные в работах [1] – [3]. Конечное поле, содержащее $k = p^m$ элементов, где p – простое число, а m – натуральное число, обозначим E_k. Кольцо многочленов переменной ξ с коэффициентами из E_k обозначим $E_k[\xi]$, а поле, полученное из E_k путем трансцендентного расширения переменной ξ обозначаем $E_k(\xi)$. Это поле состоит из дробей, числитель и знаменатель которых являются взаимнопростыми многочленами из $E_k[\xi]$. Подкольцо поля $E_k(\xi)$, состоящее из дробей, знаменатели которых не делятся на ξ, обозначим $E'_k(\xi)$. Кольцо формальных степенных рядов переменной ξ над полем E_k обозначим $R_k(\xi)$. Это кольцо содержит подкольцо, состоящее из рядов, коэффициенты которых образуют периодическую (с предпериодом) последовательность, изоморфное кольцу $E'_k(\xi)$.

Входные переменные и переменная, приписанная выходу линейного автомата принимают значения из кольца $R_k(\xi)$. Лиинейным автоматом мы называем отображение $f(x_1, x_2, \ldots, x_n)$, для которого в $E'_k(\xi)$ найдутся такие элементы μ_i, $i = 0, 1, \ldots, n$, что для любых α_i, $\alpha_i \in R_k(\xi)$, $i = 1, 2, \ldots, n$ выполнено равенство:

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

Переменная x_i этого автомата называется существенной, если $\mu_i \neq 0$, эта переменная называется непосредственной, если $\mu_i(0) \neq 0$. Через $U(f)$ будем обозначать $\{\ \mu_i \mid i = 1, 2, \ldots, n\ \}$, а через $C(f)$ будем обозначать множество с одним элементом: $C(f) = \{\ \mu_0\ \}$.

Множество всех линейных автоматов над полем E_k обозначим $\mathfrak{L}_k$. Множество $\mathfrak{L}_k$ вместе с опрерациями суперпозиции и обратной связи представляет собой класс линейных автоматов [4] над полем E_k с операциями композиции.

Для множества M линейных автоматов полагаем: $U(M) = \cup_{f \in M} U(f)$.

Наша цель найти все предполные классы [5] в классе $\mathfrak{L}_k$ для случая $m > 1$, так как случай простого поля был рассмотрен ранее в работе [6].

В дальнейшем нам понадобятся следующие подмножества линейных автоматов.

$$T_a = \{\ f(x_1, x_2, \ldots, x_n) \mid n \in \mathbb{N},\ f \in \mathfrak{L}_k,\ \text{из}$$

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0 \ \text{следует}$$

$$\left. \sum_{i=1}^{n} \mu_i(0) \cdot a + \mu_0(0) = a \ \right\},$$

где $a \in E_k$.

$$V_1 = \{\ f(x_1, x_2, \ldots, x_n) \mid n \in \mathbb{N},\ f \in \mathfrak{L}_k,$$

$$f \ \text{имеет не более одной непосредственной переменной}\ \}.$$

$$V_p = \{\ f(x_1, x_2, \ldots, x_n) \mid n \in \mathbb{N},\ f \in \mathfrak{L}_k,\ \text{и из}$$

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0 \ \text{следует}$$

$$\left. \sum_{i=1}^{n} \mu_i(0) = 1 \right\}.$$

Разложим число m в произведение различных простых чисел q_s, $s = 1, 2 \ldots, l$:

$$m = q_1^{r_1} \cdot q_2^{r_2} \ldots q_l^{r_l}. \tag{2}$$

Для каждого s, $s = 1, 2 \ldots, l$, в поле E_k содержится подполе E_{k_s} из $k_s = \frac{k}{q_s}$ элементов [7]. Положим:

$$P_s = \{ \ f(x_1, x_2, \ldots, x_n) \ \mid \ n \in \mathbb{N}, \ \ f \in \mathfrak{L}_k,$$

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

$$\mu_i(0) \in E_{k_s} \ \ i, \ \ i = 1, 2, \ldots, n \quad \}.$$

Для дроби $\mu \in E'_k(\xi)$, $\mu = \frac{u}{v}$, такой, что выполнено $\deg u \leq \deg v$, найдется целое неотрицательное число r и найдутся a, a', b, b', u', v', $s \in \mathbb{N}$, $\quad a, a' \in E_k$, $\quad b, b' \in E_k \setminus \{0\}$, $\quad u', v' \in E_k[\xi]$, $\quad \deg u' < s - 1$, $\deg v' < s - 1$, такие, что имеет место равенство:

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

Тогда положим: $\Psi_0(\mu) = \left(\frac{a}{b}, \frac{a'}{b'}\right)$.

Для каждого автоморфизма ω поля E_k определим следующие множества:

$$M_\omega^{(1)} = \Big\{ \ \mu \ \mid \ \mu \in E'_k(\xi), \ \ \mu = \frac{u}{v},$$

$$\deg u \leq \deg v, \ \ \Psi_0(\mu) = (\mu(0), \omega(\mu(0))) \ \},$$

$$M_\omega = \Big\{ \ f \ \mid \ f \in \mathfrak{L}_k, \ \ U(f) \subseteq M_\omega^{(1)} \ \Big\}. \tag{3}$$

Множество всех автоморфизмов поля E_k будем обозначать Ω.

Занумеруем все неприводимые приведенные многочлены из $E_k[\xi]$: $p_1, p_2, \ldots$ так, что $p_1 = \xi$.

Если дробь μ, $\mu \in E'_k(\xi)$, $\mu = \frac{u}{v}$ представлена в несократимом виде и для некоторого j, $j \in \{2, 3, \ldots\}$, и v не делится на p_j, то найдется, и притом однозначно многочлен u', $\deg u' \leq \deg(p_j)$, такой, что для некоторого μ' из $E'_k(\xi)$, знаменатель которой не делится на p_j, имеет место равенство:

$$\mu = u' + \xi p_j \mu'.$$

При этом положим: $\Psi_j(\mu) = u'$.

В дальнейшем будем использовать следующие множества линейных автоматов.

$$M_j = \{ \ f(x_1, x_2, \ldots, x_n) \ \mid \ n \in \mathbb{N}, \ \ f \in \mathfrak{L}_k,$$

$$f\left(x_1, x_2, \ldots, x_n\right) = \sum_{i=1}^{n} \mu_i x_i + \mu_0,$$

$$\Psi_j(\mu_i) \in E_k,\ \ i = 1, 2, \ldots, n\ \ \}\,.$$

Положим далее:

$$M_1 = \{\ \ f\left(x_1, x_2, \ldots, x_n\right)\ \ |\ \ n \in \mathbb{N},\ \ f \in \mathfrak{L}_k,$$

$$f\left(x_1, x_2, \ldots, x_n\right) = \sum_{i=1}^{n} \mu_i x_i + \mu_0,$$

$$\mu_i(\xi) - \mu_i(0) \in \xi^2 \cdot E_k'(\xi),\ \ i = 1, 2, \ldots, n\ \ \}\,.$$

Введем некоторые классы одноместныхлинейных автоматов:

$$M_0^{(1)} = \left\{\ \ \mu\ \ |\ \ \mu \in E_k'(\xi),\ \ \mu = \frac{u}{v},\ \ \deg u \le \deg v \right\},$$

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

$$M_1^{(1)} = \{\ \ \mu\ \ |\ \ \mu \in E_k'(\xi),\ \ \mu - \mu(0) \in \xi^2 \cdot E_k'(\xi)\ \ \}\,,$$

$$M_j^{(1)} = \left\{\ \ \mu\ \ |\ \ \mu \in E_k'(\xi),\ \ \mu = \frac{u}{v},\ \ (u, v) = 1,\ \ p_j\ \text{не делит}\ \ v\ \ \right\},$$

$$\tilde{M}_j^{(1)} = \left\{\ \ \mu\ \ |\ \ \mu \in E_k'(\xi),\ \ \mu = \frac{u}{v},\ \ (u, v) = 1,\ \ p_j\ \text{делит}\ \ u\ \ \right\},$$

$j = 2, 3, \ldots,$

$$R_j^e = \left\{\ \ f\ \ |\ \ f \in \mathfrak{L}_k,\ \ f\left(x_1, x_2, \ldots, x_n\right) = \sum_{i=1}^{n} \mu_i x_i + \mu_0,\right.$$

$\forall i, i = 1, 2, \ldots, n,$ если x_i — единственная существенная

переменная функции f, то $\mu_i \in M_j^{(1)}$,

в противном случае: $\left.\mu_i \in \tilde{M}_j^{(1)}\ \ \right\},$

$$R_j^r = \left\{\ \ f\ \ |\ \ f \in \mathfrak{L}_k,\ \ f\left(x_1, x_2, \ldots, x_n\right) = \sum_{i=1}^{n} \mu_i x_i + \mu_0,\right.$$

$\forall i, i = 1, 2, \ldots, n,$ если x_i — единственная непосредственная

переменная функции f, то $\mu_i \in M_j^{(1)}$,

$$\text{в противном случае: } \mu_i \in \tilde{M}_j^{(1)} \ \Big\},$$

$j = 0, 2, 3, \ldots$.

Степенью дроби μ, $\mu = \frac{u}{v}$, из $E_k(\xi)$ будем называть, как принято, число $\deg(\mu)$, равное максимуму из степеней ее числителя и знаменателя. Положим:

$$Q = \{ \ \mu \ | \ \mu \in E'_k(\xi), \ \deg(\mu) = 1, \}. \tag{4}$$

Постое трансцендентное расширение поля E_{k_s}, $s \in \{1, 2, \ldots, l\}$, элементом μ из множества Q обозначим $E_{k_s}(\mu)$. В дальнейшем мы используем множества $B_{\mu,s}$:

$$B_{\mu,s} = \Big\{ \ f \ | \ f \in \mathfrak{L}_k, \ \ f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0,$$

$$\forall i, i = 1, 2, \ldots, n, \ \ \mu_i \in E_{k_s}(\mu) \ \Big\}.$$

Нам понадобится множество $\tilde{J}_k$,

$$\tilde{J}_k = \{ \ V_1, V_p, P_s, T_a, M_\omega, M_j, R_i^e, R_i^r, B_{\mu,s} \ |$$

$$s \in \{1, 2, \ldots, l\}, a \in E_k, \omega \in \Omega, j \in \{1, 2, 3, \ldots\},$$

$$i \in \{0, 2, 3, \ldots\}, \mu \in Q\}$$

Следующее утверждение без труда доказывается индуцией по построению.

Лемма 1. *Множество $\tilde{J}_k$ состоит из замкнутых в $\mathfrak{L}_k$ классов, не совпадающих с $\mathfrak{L}_k$.*

Доказательство. Замкнутость классов V_1, V_p, T_a, M_j, R_i^e, R_i^r доказывается также, как и для аналогичных классов в случае простого поля.

Для доказательства замкнутости классов P_s, M_ω и $B_{\mu,s}$ будем использовать замыкание $K^{(1)}$ над подмножествами из $E'_k(\xi)$, которое определено в [1]. Там же показано, что для любого M, $M \subseteq \mathfrak{L}_k$, выполнены соотношения:

$$U(K(M)) \subseteq K^{(1)}(U(M)). \tag{5}$$

Нетрудно видеть, что все три операции оператора замыкания $K^{(1)}$ сохраняют множества $E'_k(\xi) \cap M_\omega^{(1)}$ и $E'_k(\xi) \cap E_{k_s}(\mu)$. Поэтому множества M_ω и $B_{\mu,s}$ являются замкнутыми классами.

Рассмотрим класс P_s. Если $\mu_i \in E'_k(\xi)$ и при этом $\mu_i(0) \in E_{k_s}$, $i = 1, 2$, то

$$(\mu_1 + \mu_2)(0) \in E_{k_s},$$

$$(\mu_1\mu_2)(0) \in E_{k_s},$$

и в случае, если к паре (μ_1, μ_2) применима операция "Об", то есть, если $\mu_2(0) = 0$, то

$$\text{Об}(\mu_1, \mu_2)(0) = \frac{\mu_1}{1 - \mu_2}(0) = \mu_1(0) \in E_{k_s}.$$

Таким образом, согласно соотношению (5), свободный член любого ряда из $U(K(P_s))$ содержится в E_{k_s}, то есть класс P_s замкнут.

Таким образом, все множества из $\tilde{J}_k$ являютяс замкнутыми классами. Для завершения доказательства леммы для каждого класса из рассматриваемого множества приведем пример линейного автомата, не содержащегося в этом классе:

$$x_1 + x_2 \notin V_1 \cup V_p \cup \left(\bigcup_i R_i^e\right) \cup \left(\bigcup_i R_i^r\right),$$

$$1 \notin T_0,$$

$$\xi x \notin \left(\bigcup_{a, a \neq 0} T_a\right) \cup \left(\bigcup_{\omega} M_\omega\right) \cup \left(\bigcup_j M_j\right),$$

пусть b — примитивный элемет поля E_k, тогда

$$bx \notin \left(\bigcup_s P_s\right) \cup \left(\bigcup_{(\mu,s)} B_{\mu,s}\right).$$

Лемма доказана.

В дальнейшем мы выделим из множества $\tilde{J}_k$ некоторое подмножество, являющееся приведенной критериальной системой в $\mathfrak{L}_k$, которое также окажется множеством всех предполные классы в $\mathfrak{L}_k$.

Удалив из множества $\tilde{J}_k$ замкнутые классы семейства $\{ B_q \mid q \in Q \}$, получим множество $\hat{J}_k$.

Лемма 2. *Для любых различных классов Θ и Θ' из множества $\hat{J}_k$ выполнено:*

$$\Theta \not\subset \Theta'. \tag{6}$$

Доказательство. Для каждого Θ, $\Theta \in \hat{J}_k$, укажем такое множество $\hat{\Theta}$, что

$$\hat{\Theta} \subset \Theta, \tag{7}$$

но для любого Θ', $\Theta' \in \hat{J}_k \setminus \{\Theta\}$, выполнено:

$$\hat{\Theta} \not\subseteq \Theta'. \tag{8}$$

Пусть b — примитивный элемент поля E_k. Положим:

$$\hat{V}_1 = \{\ \xi x_1 + \xi x_2 + 1,\ \ bx\ \},$$

$$\hat{V}_p = \{\ \xi x_1 + x_2 + 1,\ \ bx_1 + bx_2 + \cdots + bx_p + x_{p+1}\ \}.$$

Обозначим через b_s элемент поля E_{k_s}, являющийся примитивным элементом этого поля,

$$\hat{P}_s = \{\ b_s x_1 + b_s x_2,\ \ \xi x_1 + \xi x_2,\ \ 1\ \},$$

$s = 1, 2, \ldots, l$.

$$\hat{T}_a = \{\ (p-1)bx_1 + bx_2 + a,\ \ \xi x_1 + \xi x_2 + a\ \},$$

$$\hat{M}_{id} = \left\{\ bx_1 + x_2,\ \ \frac{\xi}{1+\xi^2}x_1 + \frac{\xi}{1+\xi^2}x_2,\ \ 1\ \right\},$$

$$\hat{M}_{\omega} = \left\{\ \frac{b+\omega(b)\xi}{1+\xi}x_1 + \frac{b+\omega(b)\xi}{1+\xi}x_2,\ \ \frac{\xi}{1+\xi^2}x_1 + \frac{\xi}{1+\xi^2}x_2,\ \ 1\ \right\},$$

если $\omega \in \Omega \setminus \{id\}$.

$$\hat{M}_j = \{\ (b + \xi p_j)\, x_1 + (b + \xi p_j)\, x_2,\ \ \xi p_j x_1 + \xi p_j x_2,\ \ 1\ \},$$

$j = 1, 2, \ldots,$

$$\hat{R}_0^e = \left\{\ \frac{\xi}{1+\xi}x,\ \ \frac{b}{1+\xi}x_1 + \frac{b}{1+\xi}x_2,\ \ 1\ \right\},$$

$$\hat{R}_i^e = \left\{\ \xi x,\ \ b\frac{p_i}{p_i(0)}x_1 + p_i x_2,\ \ 1\ \right\},$$

$i = 2, 3 \ldots,$

$$\hat{R}_0^r = \left\{\ \frac{\xi}{1+\xi^2}x_1 + bx_2,\ \ \frac{b}{1+\xi}x_1 + \frac{b}{1+\xi}x_2,\ \ 1\ \right\},$$

$$\hat{R}_i^r = \{\ bx_1 + \xi p_i x_2,\ \ p_i x_1 + p_i x_2,\ \ 1\ \},$$

$i = 2, 3 \ldots,$

Лемма 3. *Пусть* $M \subseteq \mathfrak{L}_k$ *и для любого* Θ, $\Theta \in \hat{J}_k$, *выполнено:*

$$M \not\subseteq \Theta. \tag{9}$$

Тогда для любого j, $j = 0, 1, 2, \dots$ справедливо:

$$U\left(K(M)\right) \not\subseteq M_j^{(1)}. \tag{10}$$

Доказательство. Рассмотрим подмножество M множества $\mathfrak{L}_k$ такое, что $\forall \Theta, \Theta \in \hat{J}_k$, справедливо (9). Соотношение (10) для $j = 1$ вытекает из определения класса M_1.

Поэтому будем рассматривать значения j из множества $\{0, 2, 3, \dots\}$. Для замыкания множества $U(M)$ по операциям сложения и умножения будем использовать обозначение $S^{(1)}\left(U(M)\right)$. По лемме 12 из работы [1] для каждого j, $j = 0, 2, 3 \dots$, соотношение (10) следует из существования μ_j, $\mu_j \in S^{(1)}(U(M))$, такого, что $\mu_j \notin \tilde{M}_j^{(1)}$ и $\mu_j(0) = 0$.

Если $U\left(M\right) \not\subseteq M_j^{(1)}$, то (10) выполнено. В противном случае, пусть $j = 0$. Из $M \not\subseteq R_0^e$ следует,что в $U(M)$ найдется μ_0', не содержащаяся в $\tilde{M}_0^{(1)}$.

Для некоторых a' и b' из E_k имеем: $\Psi_0(\mu_0') = (a', b')$, $b' \neq 0$. Если $a' = 0$, то дробь μ_0' искомая и соотношение (10) имеет место. Если $a' \neq 0$, то обозначим через $g'(z)$ ненулевой многочлен из $E_p[z]$ с минимальной степенью, для которого $g'(a') = 0$. Если при этом $g'(b') \neq 0$, то искомым является элемент $g'(\mu')$ из $S^{(1)}(U(M))$.

В противном случае, из соотношений $M \not\subseteq P_s$, $s = 1, 2, \dots, l$, следует, что для некоторого примитивного элемента a поля E_k в $U(K(M))$ найдется элемент μ такой, что для некоторого b, $b \in E_k$, справедливо: $\Psi_0(\mu) = (a, b)$. Если $b = 0$, то через r обозначим такое натуральное число, что $a^r = a'$. Тогда дробь $\mu_0' - \mu^r$ — искомая. Если же $b \neq 0$ и b не сопряжено с a, рассмотрим ненулевой многочлен $g(z)$ над E_p степени m такой, что $g(a) = 0$. Если $g(b) \neq 0$, то дробь $g(\mu)$ — искомая. В противном случае, через ω обозначим автоморфизм поля E_k, переводящий элемент a в элемент b. Из соотношения $M \not\subseteq M_\omega$ следует, что в $U(M)$ найдется такое μ'', что для некоторого натурального i выполнено равенство $\Psi_0\left(\mu''\right) = \left(a^i, c\right)$ и $c \neq b^i$. Тогда дробь $\mu^i - \mu''$ является искомой. Таким образом, случай $j = 0$ разобран.

Пусть $j \in \{2, 3, \dots\}$. Множество $U(K(M))$, как было сказано ранее, содержит элемент μ такой, что $a = \mu(0)$ является примитивным элементом поля E_k. Имеем соотношение: $\mu \in M_j^{(1)} \setminus \tilde{M}_j^{(1)}$. Пусть $\Psi_j(\mu) = u$

таково, что $u = a$. Ввиду соотношения $M \not\subseteq M_j$ в M содержится элемент μ'_j такой, что $\Psi_j(\mu') = u'$, $u' \notin E_k$. Если $\mu'(0) = 0$, то дробь μ' — искомая. В противном случае, найдется натуральное число r такое, что $a^r = \mu'(0)$. Тогда дробь $\mu' - \mu^r$ является искомой. Если $u \neq a$, но u делится на p_j, то рассмотрим дробь μ'', такую, что $\mu'' \in U(M) \setminus \tilde{M}_j^{(1)}$, которая существует ввиду соотношения $M \not\subseteq R_j^e$. Найдется натуральное число r' такое, что $\mu''(0) = a^{r'}$. Тогда искомая дробь: $\mu'' - \mu^{r'}$.

Осталось рассмотреть случай, когда многочлен u не является элементом поля E_k и не делится на многочлен p_j. В этом случае если бы многочлены u и u^k давали бы одинаковые остатки от деления на многочлен $\xi \cdot p_j$, то многочлен $u^k - u$ делился бы на p_j. Тогда в поле Γ_j, являющемся алгебраическим расширением поля E_k элементом z таким, что $p_j(z) = 0$, нашелся бы элемент, не содержащийся в поле E_k, порядок которого делил число k. Но [7], в поле Γ_j все элементы, не содержащиеся в E_k, имеют порядок больше k. Отсюда следует, что дробь $\mu^k - \mu$ в последнем рассматриваемом случае является искомой.

Лемма 3 доказана.

Лемма 4. *Если Θ – предполный класс в $\mathfrak{L}_k$, не содержащийся ни в одном из замкнутых классов системы $\hat{J}_k$, то*

$$E_k \not\subseteq E_p\left(U(\Theta)\right). \tag{11}$$

Доказателство. Рассмотрим предполный класс Θ в $\mathfrak{L}_k$, не содержащийся ни в одном из классов множества $\hat{J}_k$. Если соотношение (11) не выполнено, то по теореме Люрота [8] поле $E_p(U(\Theta))$ является простым расширением поля E_k. Поэтому найдется $\mu \in E_k(\xi)$, что справедливо равенство:

$$E_p(U(\Theta)) = E_k(\mu). \tag{12}$$

Не ограничивая общности рассуждений, будем предполагать, что $\mu \in \xi \cdot E'_k(\xi)$. Отсюда и из равенства (12) следует, что $U(\Theta)$ содержится в $K^{(1)}\left(\{\mu, E_k\}\right)$, где оператор замыкания $K^{(1)}$ определен в [1].

Предположим, что $\deg \mu > 1$. Тогда $\mu = \xi\frac{u}{v}$, $u, v \in E_k[\xi]$, $(u, v) = 1$. Если $\deg u \geq 1$, то для некоторого i, $i \in \{1, 2, \dots\}$, получаем включение $\Theta \subseteq M_i$, что противоречит предположению. Если $u \in E_k \setminus \{0\}$ и $\deg v = k' > 1$, то для некоторых a_1, b_0, b_k из $E_k \setminus \{0\}$ имеем: $\mu = \xi\frac{a_1}{b_0 + \xi v' + b_k\xi^k}$, $\deg v' < k' - 1$. Поэтому $\Psi_0(\mu) = (0, 0)$ и $\Theta \subseteq M_{Id}$, где через Id обозначен тождественный автоморфизм поля E_k. Снова получаем противоречие.

Таким образом, $\deg(\mu) = 1$, и, как нетрудно видеть,

$$E_k(\mu) = E_k(\xi).$$

Отсюда, из леммы 3 и теорем 2 и 4 работы [1] вытекает полнота Θ в $\mathfrak{L}$, что противоречит предположению о том, что Θ — предполный класс в $\mathfrak{L}$.

Лемма 4 доказана.

Лемма 5. *Пусть Θ – предполный класс в $\mathfrak{L}_k$, не содержащийся ни в одном из замкнутых классов системы $\hat{J}_k$, и пусть*

$$k_0 = \max_{k'} \{E_{k'} \subseteq E_p(U(\Theta))\}, \tag{13}$$

$k_0 = p^{m_0}$, $m : m_0 = m_1$ и $E_p(a) = E_k$. Тогда для некоторых ω_i, $\omega_i \in E_p(U(\Theta))$, $i = 0, 1, \ldots, m_1 - 1$, выполнено равенство:

$$\xi = \sum_{i=0}^{m_1-1} \omega_i \cdot a^i. \tag{14}$$

Доказательство. Рассмотрим Θ – предполный класс в $\mathfrak{L}_k$, такой, что $\forall \Theta' \in \hat{J}_k$ выполнено: $\Theta \neq \Theta'$. Из леммы 4 следует, что

$$K(\Theta \cup \{a \cdot x\}) = \mathfrak{L}_k.$$

Поэтому

$$E_p(U(\Theta) \cup \{a\}) = E_k(\xi).$$

Согласно [9], $E_k(\xi)$ является линейным пространством над $E_p(U(\Theta))$, порожденным элементами множества $\{a^0, a, a^2, ..., a^{m_1-1}\}$. Отсюда следует равенство (14). Лемма 5 доказана.

Лемма 6. *Пусть Θ – предполный класс в $\mathfrak{L}_k$, не содержащийся ни в одном из замкнутых классов системы $\hat{J}_k$ и выполнено* (13)*. Тогда найдется μ, $\mu \in U(\Theta)$, такое, что*

$$E_{k_0}(\mu) = E_p(U(\Theta)), \tag{15}$$

$$\deg(\mu) = 1 \tag{16}$$

и E_{k_0} – максимальное подполе в E_k.

Доказательство. По лемме 5 в $E_p(U(\Theta))$ найдутся такие ω_i, $i = 0, 1, \ldots, m_1 - 1$, что многочлен $z - \sum_{i=0}^{m_1-1} \omega_i \cdot a^i$ имеет корень $z = \xi$.

Пусть $\omega_i = \frac{u_i}{v_i}$ – несократимые дроби, $u_i \in E_k[\xi]$, $v_i \in E_k[\xi]$, $i = 0, 1, ..., m_1 - 1$. Среди коэффициентов ω_i, $i = 0, 1, \ldots, m_1 - 1$ найдется такой ω_{i_0}, который зависит от ξ, иначе бы ξ, согласно равенству (14), содержалась бы в E_k.

Многочлен $\omega_{i_0} \cdot v_{i_0}(z) - u_{i_0}(z)$ переменной z имеет корень $z = \xi$. Нетрудно видеть, что он делится на многочлен $z - \sum_{i=0}^{m_1-1} \omega_i \cdot a^i$, так как в противном случае элементы поля a^0, a^1,..., a^{m_1-1}, были линейно зависимы над полем $E_p(U(\Theta))$.

Через $\tilde{v}$ обозначим наименьшее общее кратное многочленов v_0, v_1, $\ldots$, v_{m_1-1}.

Многочлен $f(\xi)$, $f(\xi) = u_{i_0} \cdot v_{i_0} - u_{i_0} \cdot v_{i_0}$ переменной ξ делится на многочлен $g(\xi)$, $g = \tilde{v}\left(z - \sum_{i=0}^{m_1-1} \omega_i \cdot a^i\right)$ этой же переменной [8]. Поэтому $\deg_\xi(f(\xi)) \geq \deg_\xi(g(\xi))$. С другой стороны $\deg_\xi(f(\xi)) \leq \deg_\xi(g(\xi))$. Отсюда, $\deg_\xi(f(\xi)) = \deg_\xi(g(\xi))$. Поэтому для некоторого многочлена из $h(z)$, $h(z) \in E_k[z]$, получаем:

$$f(\xi) = h(z) \cdot g(\xi).$$

Разделив многочлен $\omega_{i_0} \cdot v(z) - u(z)$ переменной z на $h(z)$, получим многочлен первой степени от z с коэффициентами из $E_k(\omega_{i_0})$. Отсюда следует, что найдутся такие дроби ω_i', $\omega_i' \in E_{m_1}(\omega_{i_0})$, $i = 0, 1, \ldots, m_1 - 1$, что

$$\xi = \sum_{i=0}^{m_1-1} \omega_i' \cdot a^i.$$

Таким образом,

$$(E_k(\xi) : E_p(U(\Theta))) = (E_k(\xi) : E_{k_0}(\omega_{i_0})) = m_1 \tag{17}$$

и при этом

$$E_{k_0}(\omega_{i_0}) \subseteq E_p(U(\Theta)).$$

Отсюда для $\mu = \omega_{i_0}$ следуетравенство (15).

Из равенства (17), леммы 4 и равенств

$$(E_k(\xi) : E_{k_0}(\mu)) = (E_k(\xi) : E_k(\mu)) \cdot (E_k : E_{k_0}),$$

$$(E_k : E_{k_0}) = m_1$$

получаем:

$$(E_k(\xi) : E_k(\mu)) = 1.$$

Далее, принимая во внимание, что

$$(E_k(\xi) : E_k(\mu)) = \deg(\mu),$$

получаем (16).

Если E_{k_0} не является максимальным подполем в E_k, то для некоторого максимального подполя $E_{k'}$ поля E_k имеем:

$$E_{k_0}(\mu) \subset E_{k'}(\mu) \subset E_k(\xi),$$

$$E_{k_0}(\mu) \neq E_{k'}(\mu) \neq E_k(\xi),$$

поэтому Θ не является предполным классом в $\mathfrak{L}_k$, что противоречит условию леммы.

Лемма 6 доказана.

Следствие 1. *Если Θ — предполный класс в $\mathfrak{L}_k$, не содержащийся ни в одном из замкнутых классов системы $\hat{J}_k$, то для некоторых μ и s, $\mu \in Q$, $s \in \{1, 2, \ldots, l\}$, выполнено: $\Theta = B_{\mu,s}$.*

Отсюда получаем следующее утверждение.

Теорема 1. *Множество замкнутых классов $\tilde{J}_k$ является критериальной системой [5] в $\mathfrak{L}_k$, то есть для любого подмножества M множества $\mathfrak{L}_k$ его полнота в $\mathfrak{L}_k$ равносильна невключению в каждый замкнутый класс множества $\tilde{J}_k$.*

Доказательство. Если множество линейных автоматов M не является полным в $\mathfrak{L}_k$, и не содержится ни в одном из замкнутых классов множества $\hat{J}$, то M содержится в некотором предполном классе, которое, согласно следствию 1, совпадает с некоторым $B_{\mu,s}$. Поэтому любое множество, не являющееся полным, содержится в некотором классе множества $\tilde{J}$.

С другой стороны, множество линейных автоматов M, являющееся полным, не может содержаться ни в одном из классов множества $\tilde{J}$, так как каждый класс этого множества по лемме 1 замкнут и не совпадает с $\mathfrak{L}_k$.

Теорема 1 доказана.

Далее из множества $\tilde{J}$ выделим подмножество, являющееся приведенной критериальной системой, то есть системой замкнутых классов,

удаляя из которой любой класс, получаем множество классов, не являющееся критериальной системой.

С учетом разложения (2), как известно [7], в поле E_k содержится l максимальных подполей: E_{k_i}, $i = 1, 2, \ldots, l$, при этом $k_i = \frac{k}{q_i}$.

Автоморфизм ω поля E_k будем называть минимальным, если он не является тождественным и сохраняет некоторое максимальное подполе поля E_k.

Пару (μ, s), где $\mu \in Q$, $s \in \{1, 2, \ldots, l\}$, будем называть допустимой, если $\mu(0) \notin E_{k_s}$, а также, если $\mu \in M_0^{(1)}$ и $\Psi(\mu) = (a, b)$, то $\omega(a) \neq b$ для любого минимального автоморфизма ω поля E_k, сохраняющего подполе E_{k_s}.

Нетрудно видеть, что для любой допустимой пары (μ, s) поле $E_{k_s}(\mu)$ является собственным подполем поля $E_k(\xi)$.

Положим:

$$J'_k = \{\ B_{\mu,s} \mid \text{пара } (\mu, s) \text{ допустима } \},$$

$$J_k = \hat{J}_k \cup J'_k.$$

Теорема 2. *Множество замкнутых классов J_k является приведенной критериальной системой в $\mathfrak{L}_k$.*

Для доказательства этой теоремы нам понадобятся некоторые вспомогательные утверждения.

Лемма 7. *Для любого замкнутого класса Θ из множества $\tilde{J}_k \setminus J_k$ найдется такой Θ' из J_k, что выполнено включение:*

$$\Theta \subseteq \Theta'.$$

Доказательство леммы 7.

Рассмотрим Θ, $\Theta \in \tilde{J}_k \setminus J_k$. Тогда для некоторых μ и s, $\mu \in Q$, $s \in \{1, 2, \ldots, l\}$, выполнено:

$$\Theta = B_{\mu,s}.$$

При этом имеет место один из следующих двух случаев.

Случай 1. $\mu(0) \in E_{k_s}$.

Случай 2. $\mu \in M_0^{(1)}$ и для некоторого минимального автоморфизма ω поля E_k, сохраняющего элементы подполя E_{k_s}, выполнено: $\Psi(\mu) = (a, \omega(a))$.

Заметим, что в случае 1 выполнено включение $\{\mu, E_{k_s}\} \subset P_s$, поэтому $B_{\mu,s} \subseteq P_s$, а в случае 2 имеет место: $\{\mu, E_{k_s}\} \subset M_\omega$, поэтому $B_{\mu,s} \subseteq M_\omega$.

Лемма 7 доказана.

Из последней леммы вытекает следующее утверждение.

Следствие 2. *Множество J_k является критериальной системой замкнутых классов в $\mathfrak{L}_k$.*

Далее продолжим обоснование приведенности критериальной системы J_k.

Лемма 8. *Если пары (μ, s) и (μ', s') являются допустимыми и*

$$E_{k_{s'}}\left(\mu'\right) \subseteq E_{k_s}\left(\mu\right), \tag{18}$$

то

$$s = s', \tag{19}$$

$$E_{k_s}\left(\mu\right) = E_{k_{s'}}\left(\mu'\right) \tag{20}$$

и для некоторых b_j, $b_j \in E_{k_s}$, $j = 1, 2, 3, 4$, выполнены соотношения:

$$\mu' = \frac{b_1 + b_2\mu}{b_3 + b_4\mu}. \tag{21}$$

Доказательство. Пусть для допустимых пар (μ, s) и (μ', s') имеет место включение (18). Тогда $E_{k_{s'}} \subseteq E_{k_s}$, а из максимальности подполей E_{k_s} и $E_{k_{s'}}$ в E_k следует, что $E_{k_{s'}} = E_{k_s}$. Поэтому равенство (19) справедливо.

Отсюда, из равенства

$$\left(E_k(\xi) : E_{k_s}(\mu')\right) = \left(E_k(\xi) : E_{k_s}(\mu)\right) = q_s$$

и включения (18) получаем равенство (20).

Для некоторых взаимнопростых многочленов $u(\xi)$ и $v(\xi)$ из $E_{k_s}[\xi]$ выполнено:

$$\mu' = \frac{u(\mu)}{v(\mu)}.$$

Если степень дробь $\eta(\xi) = \frac{u(\xi)}{v(\xi)}$ равна r, то

$$\left(E_{k_s}(\mu) : E_{k_s}(\mu')\right) = \left(E_{k_s} : E_{k_s}\right) \cdot r,$$

откуда и из равенства (20) получаем $r = 1$, поэтому выполнено равенство (21).

Лемма 8 доказана.

Следствие 3. *Множество замкнутых классов J'_k является приведенным.*

Из этого следствия и леммы 2 получаем приведенность каждого из множеств J'_k и $\hat{J}_k$. Теперь нужно доказать приведенность объединения этих множеств.

Лемма 9. *Для любого Θ, $\Theta \in J'_k$, и любого Θ', $\Theta' \in \hat{J}_k$, выполнено:*

$$\Theta \not\subseteq \Theta'$$

и

$$\Theta' \not\subseteq \Theta.$$

Доказательство. Рассмотрим класс $B_{\mu,s}$ для допустимой пары (μ, s). Через b обозначим примитивный элемент поля E_{k_s}. Для множества $\hat{B}_{\mu,s}$,

$$\hat{B}_{\mu,s} = \{\ \mu x,\ \ bx_1 + bx_2\ \ , 1\ \}$$

имеем: $\hat{B}_{\mu,s} \subset B_{\mu,s}$, но для любого Θ', $\Theta' \in \hat{J}_k$, выполнено: $\hat{B}_{\mu,s} \not\subseteq \Theta'$. Таким образом, замкнутый класс $B_{\mu,s}$ не содержится ни в каком классе из множества $\hat{J}_k$.

С другой стороны, обозначив через b примитивный элемент поля E_k, заметим, что класс $B_{\mu,s}$ не содержит ни одну из функций следующих функций:

$$bx,$$

$$bx_1 + (1-b)x_2,$$

$$(\mu - \mu(0))x + a, \quad \forall a \in E_k,$$

$$\frac{b\xi}{1+\xi^2}x_1 + \frac{\xi}{1+\xi^2}x_1,$$

$$b\xi p_i x_1 + \xi p_i x_2, \quad i = 1, 2, \ldots,$$

$$bp_i x_1 + p_i x + 2, \quad i = 1, 2, \ldots.$$

Для обоснования этого достаточно двух свойств класса $B_{\mu,s}$:

1) $E_k \not\subseteq U(B_{\mu,s})$;

2) Если $\mu \in U(B_{\mu,s})$, $\mu' \in U(B_{\mu,s})$ и $\frac{\mu}{\mu'} \in E'_k(\xi)$, то $\frac{\mu}{\mu'} \in U(B_{\mu,s})$.

При этом,

$$bx \in V_1,$$

$$bx_1 + (1-b)x_2 \in V_p,$$

$$(\mu - \mu(0))x \in P_s, \quad \forall s, s \in \{1, 2, \dots, l\},$$

$$(\mu - \mu(0))x + a \in T_a, \quad a \in E_k,$$

$$\frac{b\xi}{1+\xi^2}x_1 + \frac{\xi}{1+\xi^2}x_1 \in M_\omega \cap R_0^e \cap R_0^r, \quad \forall \omega \in \Omega,$$

$$b\xi p_i x_1 + \xi p_i x_2 \in M_i, \quad \forall i \in \{1, 2, \dots\},$$

$$bp_i x_1 + p_i x_2 \in R_i^e \cap R_i^r, \quad \forall i \in \{2, 3, \dots\}.$$

Таким образом, лемма 9 доказана.

Используя приведенность множества J_k и ее критериальность, согласно следствию 2, нетрудно получить следующий результат.

Теорема 3. *Множество J_k состоит из предполных в $\mathfrak{L}_k$ классов и каждый предполный в $\mathfrak{L}_k$ класс содержится в множестве J_k.*

Решение задачи нахождения всех предполных классов в $\mathfrak{L}_k$ позволяет построить полиномиальный алгоритм проверки полноты конечных систем линейных автоматов над полем E_k.

Пусть имеется множество M, $M \subset \mathfrak{L}_k$, $|M| < \infty$, причем каждый автомат f из M задан набором коэффициентов при переменных и константной частью $C(f)$.

Шаг 1. Проверяем включения:

$$M \subset V_1,$$

$$M \subset V_p,$$

$$M \subset P_s, \quad s = 1, 2, \dots l,$$

$$M \subset T_a, \quad a \in E_k.$$

Если хотя-бы одно из эих включений выполнено, то множество M не является полным в $\mathfrak{L}_k$, алгоритм заканчивает работу.

Шаг 2. Проверяем, верно ли включение:

$$U(M) \subset M_0^{(1)}.$$

Если нет, то переходим к шагу 4.

Шаг 3. Находим множество

$$\Psi_0(M) = \{\ \Psi_0(\mu)\ \mid\ \mu \in U(M)\ \}.$$

Пусть a — какой-либо примитивный элемент поля E_k. Каждый сопряженный к a элемент b поля E_k порождает автоморфизм ω поля E_k такой, что $\omega(a) = b$. При этом сопряженные к a элементы ищутся как корни минимального многочлена, корнем которого является a. Таким образом, количество рассматриваемых автоморфизмов ограничено числом m [8]. Для каждого автоморфизма ω проверяем включение

$$\Psi_0(M) \subseteq M_\omega.$$

Если хотя бы одно из включений выполнено, то M не является полным в $\mathfrak{L}_k$, алгоритм заканчивает работу.

Шаг 4. Находим наибольший общий делитель D_1 числителей дробей из множества U',

$$U' = \{\ \mu - \mu(0)\ \mid\ \mu \in U(M)\ \}.$$

Если $\deg(D_1) > 1$, то множество M не является полным в $\mathfrak{L}_k$ и алгоритм заканчивает работу.

Шаг 5. Находим наибольший общий делитель D_2 числителей дробей из множества U^e,

$$U^e = \{\ \mu\ \mid\ \text{в}\ M\ \text{содержит автомат, для разложения (1) которого}$$

$$\text{найдется}\ \ i\ \ \text{такое, что}\ \ \mu_i = \mu\ \ \text{и}$$

$$x_i\ \ \text{не является единственной существенной переменной}\ \ f\}.$$

Находим наибольший общий делитель D_3 числителей дробей из множества U^r,

$$U^r = \{\ \mu\ \mid\ \text{в}\ M\ \text{содержит автомат, для разложения (1) которого}$$

$$\text{найдется}\ \ i\ \ \text{такое, что}\ \ \mu_i = \mu$$

$$\text{и}\ \ x_i\ \ \text{не является единственной непосредственной переменной}\ \ f\}.$$

Наименьшее общее кратное знаменателей дробей из $U(M)$ обозначим K_1. Для $i = 2, 3$ наибольший общий делитель D_i и K_1 обозначим D'_i. Если хотя бы для одного i, $i \in \{2, 3\}$, выполнено: $D_i/D'_i \notin E_k$, то $K(M) \neq \mathfrak{L}_k$ и алгоритм заканчивает работу.

Шаг 6. Этот шаг выполняется путем перебора всех допустимых пар (μ, s). Количество таких пар ограничено сверху числом $l \cdot k^3$. Две пары (μ, s) и (μ', s) назовем эквивалентными, если $B_{\mu,s} = B_{\mu',s}$.

Далее, выбирая по одному представителю (μ, s) из каждого класса эквивалентности, выполняем проверку включения $M \subset B_{\mu,s}$. Эта проверка может быть выполнена следующим образом. Сначала выражаем ξ несократимой дробью $\frac{u}{v}$, где u и v — многочлены из кольца $E_k[\mu]$, то есть многочлены переменной μ с коэффициентами из E_k. Далее, для μ' из M проверка включения $\mu' \in B_{\mu,s}$ заключается в подстановке дроби $\frac{u}{v}$ вместо ξ в μ', приведению полученного выражения к виду $\frac{u'}{v'}$, где $u', v' \in E_k[\mu]$ и $v'(0) = 1$. Если при этом оказалось, что все коэффициенты u' и v' содержатся в E_{k_s}, то имеем: $\mu' \in B_{\mu,s}$.

Понятно, что при реализации алгоритма проверку на эквивалентность пар можно не проводить.

Если нашлась такая допустимая пара (μ, s), что $U(M) \subseteq B_{\mu,s}$, то M не является полным в $\mathfrak{L}_k$. Алгоритм заканчивает работу с отрицательным результатом. В противном случае, алгоритм заканчивает работу с положительным результатом.

Для упрощения реализации алгоритма и оптимизации времени ее работы проиндексируем элементы поля E_k числами $0, 1, \ldots, k-1$. Для элементов поля E_k, используя индексы, составим таблицы сложения, умножения, возведения в степень до степени $k - 1$.

Выберем некоторый элемент b поля E_k, являющийся примитивным для этого поля. Для упрощения реализации алгоритма и оптимизации времени его работы проиндексируем элементы поля E_k: элемент 0 индексируем числом 0, каждый ненулевой элемент a индексируем степенью i такой, что $1 \leq i \leq k - 1$ и $b^i = a$. Для элементов поля E_k, используя индексы, составим таблицы сложения, умножения, возведения в степень до степени $k - 1$, таблицу принадлежности максимальным подполям P_s, $s = 1, 2, \ldots, l$. Для каждого элемента сопряженного с b составим также таблицу индексов степеней этого элемента от 1 до $k - 1$.

Также заранее заготовим выражения ξ через каждую из дробей μ первой степени, для которой найдется s, что μ входит в допустимую пару (μ, s).

В качестве параметров для оценки времени работы этого алгоритма выберем следующие:
r — количество функций в множестве M, проверяемом на полноту;
n — максимальное количество переменных в функциях множества M;
d — максимальная степень дробей из множества $U(M)$, при этом, как

принято, $deg\left(\frac{u}{v}\right) = \max(\deg u, \deg v)$;
k — как и ранее, количество элементов конечного поля;
l — количество максимальных подполей в поле E_k.

Несложный анализ приводит к следующей теореме.

Теорема 4. *Полученный алгоритма проверки полноты конечных подмножеств линейных автоматов может быть реализован с временной сложностью* $O\left(rnd^2k^3l\right)$.

Доказательство.

Нетрудно видеть, что шаги 1-3 алгоритма могут быть реализованы с временной сложностью $O(rnk)$, шаги 4 и 5 — с временной сложностью $O\left(rnd^2\right)$, а шаг 6, с временной сложностью $O\left(rnd^2k^3l\right)$.

Теорема 4 доказана.

Список литературы

[1] Часовских, А.А. Проблема полноты для класса линейно-автоматных функций / А. А. Часовских // Дискретная математика. — 2015. — Т. 27, № 2. — С. 134–151.

[2] Часовских, А.А. Критериальные системы в классах линейно-автоматных функций над конечными полями / А. А. Часовских // Интеллектуальные системы. Теория и приложения. — 2015. — Т. 19, вып. 3. — С. 195–207.

[3] Часовских, А.А. Проблема полноты в классах линейных автоматов / А. А. Часовских // Интеллектуальные системы. Теория и приложения. — 2018. — Т. 22, вып. 2. — С. 151–154.

[4] Гилл, А. Линейные последовательные машины / А. Гилл. — М.: Наука, 1974. — 288 с.

[5] Кудрявцев, В. Б. Введение в теорию автоматов / В. Б. Кудрявцев, С. В. Алешин, А. С. Подколзин. — М.: Наука, 1985. — 320 с.

[6] Часовских, А. А. Условия полноты линейно-р-автоматных функций / А. А. Часовских // Интеллектуальные системы. Теория и приложения. — 2014. — Т. 18, вып. 3. — С. 203–252.

[7] Лидл, Р. Конечные поля: в 2 т. / Р. Лидл, Г. Нидеррайтер. — М.: Мир, 1988. — 2 т.

[8] Ван дер Варден, Б. Л. Алгебра / Б. Л. Ван дер Варден. — М.: Наука, 1976. — 648 с.

[9] Зарисский, О. Коммутативная алгебра: в 2 т. / О. Зарисский, П. Самюэль. —М.: ИЛ, 1963. — 2 т.

Reduced criterial system of are precomplete classes in linear automata classes over finite fields

Chasovskikh A.A.

The sets of all precomplete classes in the classes of linear automata over finite fields are found, which are reduced criteria systems in these classes.

Keywords: finite automaton, linear automaton, composition operations, superposition operations, feedback, completeness problem, precomplete class, criterial system, reduced criterial system, adder, delay.