О классах передаточных функций линейных автоматов

Часовских А.А.

Для классов передаточных функций линейных автоматов над конечным полем с операциями, индуцированными операциями композиции над этими автоматами, найдены все максимальные подалгебры.

Ключевые слова: конечный автомат, линейный автомат, передаточная функция, операции композиции, обратная связь, полнота, замкнутый класс, предполный класс, конечное поле.

Обозначения, которые не введены в этой работе, можно найти в [6] — [8]. Как и в этих работах, линейный автомат f над конечным полем E_k мы отождествляем с функцией, переменные которой принимают значения из $R_k(\xi)$, и для некоторых дробей μ_i из $E'_k(\xi)$, $i = 0, 1, \ldots, n$, выполнено:

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

В книге [2] коэффициенты μ_i, $i \in \{1, 2, \ldots, n\}$, называются передаточными функциями линейного автомата f.

Как следует из [6], операции композиции в классе линейных автоматов индуцируют оператор замыкания K^1 в классе передаточных функций $E'_k(\xi)$, состоящий из операций сложения, умножения и частичной операции «fb», причем для пары дробей μ_i, $i = 1, 2$, значение $\mathrm{fb}(\mu_1, \mu_2)$ определено в точности тогда, когда $\mu_2 \in \xi E'_k(\xi)$, и в этом случае имеем:

$$\mathrm{fb}(\mu_1, \mu_2) = \frac{\mu_1}{1 - \mu_2}.$$

В настоящей работе мы найдем все предполные [3] (максимальные) подклассы в $E'_k(\xi)$, рассматриваемом вместе с оператором замыкания K^1. Сначала в $E'_k(\xi)$ мы выделим некоторые подмножества. Положим:

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

$$R_0^{(1)} = \left\{ \ \mu \ \mid \ \mu \in E_k'(\xi), \ \ \mu = \frac{u}{v}, \ \ \deg u < \deg v \ \right\}.$$

Число k является степенью некоторого простого числа p, $k = p^m$. Множество автоморфизмов Ω_k поля E_k содержит $\log_p k = m$ элементов [5]. Для каждого ω, $\omega \in \Omega$, в $E_k'(\xi)$ содержится множество $M_{0,\omega}$,

$$M_{0,\omega}^{(1)} = \left\{ \ \mu \ \mid \ \mu = \frac{u}{v}, \ \ \deg u \le \deg v \ \ \mu(1/\xi)(0) = \omega(\mu(0)) \ \right\}.$$

Как указано в [6], между множеством W_k максимальных подполей поля E_k и множеством простых делителей числа $\log_p k$ имеется биективное соответствие. Положим:

$$P_\Delta^{(1)} = \left\{ \ \mu \ \mid \ \mu \in E_k'(\xi), \ \ \mu(0) \in \Delta \ \right\},$$

$\Delta \in W_k$.

Множество приведенных неприводимых многочленов кольца $E_k[\xi]$, не включающее только многочлен ξ, обозначим I_k. Для заданного p, $p \in I_k$, множество несократимых дробей из $E_k'(\xi)$, числители которых делятся на p, обозначим $R_p^{(1)}$.

Для дроби μ из $E_k'(\xi)$, знаменатель которой не делится на некоторый p, $p \in I_k$, единственным образом определен многочлен u степени меньшей $\deg p$, удовлетворяющий для некоторого μ', $\mu' \in E_k'(\xi)$, равенству

$$\mu = u + p\mu'.$$

Многочлен u при этом будем обозначать $\mathrm{rest_p}(\mu)$.

Положим:

$$M_{p,\omega}^{(1)} = \left\{ \ \mu \ \mid \ \mu = \frac{u}{v}, \ \ (u,v) = 1, \ \ \mathrm{rest_p}(\mu) = \omega(\mu(0)) \ \right\},$$

$p \in I_k$, $\omega \in \Omega$.

Нам понадобится следующее множество:

$$J_k^{(1)} = \left\{ \ M_1^{(1)}, \ R_0^{(1)}, \ M_{0,\omega}^{(1)}, \ P_\Delta^{(1)}, \ R_p^{(1)}, \ M_{p,\omega}^{(1)} \ \mid \right.$$
$$\left. \omega \in \Omega, \ \ \Delta \in W_k, \ \ p \in I_k \ \right\}.$$

Имеет место:

Теорема 1. *Множество $J_k^{(1)}$ состоит из максимальных подклассов $E_k'(\xi)$ и содержит все его максимальные подклассы.*

Тождественный автоморфизм поля E_k обозначим id. Для случая $k = p$, то есть для простого поля, имеем:

$$J_k^{(1)} = \left\{ \ M_1^{(1)}, \ R_0^{(1)}, \ M_{0,\mathrm{id}}^{(1)}, \ P_1^{(1)}, \ R_p^{(1)}, \ M_{p,\mathrm{id}}^{(1)} \ \mid \ p \in I_k \ \right\}.$$

что совпадает с результатами работы [7].

Для доказательства теоремы нам понадобятся вспомогательные утверждения. Пусть F — некоторое подполе в $E_k(\xi)$ и $M \subseteq E_k(\xi)$. Поле, полученное расширением F путем присоединения элементов множества M, обозначаем $F(M)$ [5]. Для одноэлементного множества вместо $F(\{\mu\})$ используем более короткое обозначение $F(\mu)$. Собственное подполе поля F называется максимальным, если оно не содержится в другом собственном подполе этого поля.

Лемма 1. *Если множество M, $M \subseteq E'_k(\xi)$, не содержится ни в одном Θ, $\Theta \in J_k^{(1)}$, то M не содержится ни в одном максимальном подполе поля $E_k(\xi)$.*

Доказательство леммы. Пусть $M \subseteq E'_k(\xi)$ и $\forall \Theta$, $\Theta \in J_k^{(1)}$, имеет место:

$$M \not\subseteq \Theta.$$

Рассмотрим какое-либо максимальное подполе F поля $E_k(\xi)$. Пусть

$$E_k \subseteq F. \tag{1}$$

Тогда по теореме Люрота [1] для некоторого μ, $\mu \in E_k(\xi)$, имеем: $F = E_k(\mu)$.

Если $\mu \in E_k$, то F не является максимальным подполем поля $E_k(\xi)$, так как

$$F \subsetneq E_k\left(\xi^2\right) \subsetneq E_k(\xi).$$

Если $\deg \mu = 1$, то, как не трудно видеть, $F = E_k(\xi)$, и F не является максимальным подполем поля $E_k(\xi)$.

Таким образом, $\deg \mu > 1$, и, не ограничивая общности рассуждений, будем предполагать, что $\mu \in \xi E'_k(\xi)$.

Тогда для некоторых многочленов u и v из $E_k[\xi]$ имеем: $\mu = \xi \frac{u}{v}$, $\max(\deg \xi u, \deg v) > 1$.

Если $\deg u \geq 1$, то для некоторого p, $p \in I_k$, выполнено включение:

$$\{ \ E_k, \ \mu \ \} \subset M_{p,\mathrm{id}}^{(1)}.$$

Поэтому, как не трудно видеть,

$$F \cap E'_k(\xi) \subseteq M^{(1)}_{p,\mathrm{id}},$$

откуда следует, что

$$M \not\subseteq F. \tag{2}$$

Если $\deg u = 0$, то $\deg v > 1$ и

$$F \cap E'_k(\xi) \subseteq M^{(1)}_{0,\mathrm{id}},$$

откуда вытекает (2).

Таким образом, случай (1) рассмотрен.

Пусть включение (1) не имеет места. Известно [5], что в $E_p[z]$ найдется неприводимый многочлен $f(z)$, для корня a которого, имеем:

$$E_p(a) = E_k.$$

Обозначим через $E_{k'}$ поле $E_k \cap F$. Рассмотрим ненулевой приведенный многочлен минимальной степени $g(z)$, $g(z) \in F[z]$, имеющий корень $z = a$. Нетрудно видеть, что $g(z)$ делит $f(z)$. Так как многочлена $f(z)$ имеет в поле E_k ровно m корней a^{p^0}, a^{p-1}, a^{p^2}, $\ldots$, $a^{p^{m-1}}$, то все коэффициенты многочлена $g(z)$ содержатся в $E_{k'}$. Если $E_{k'}$ не является максимальным подполем поля E_k, то найдется такое поле $E_{k''}$, что выполнены соотношения:

$$E_{k'} \subsetneq E_{k''} \subsetneq E_k.$$

В соответствии с [4], степенью расширения поля E над его подполем E' называется размерность E как линейного пространства над E', которая обозначается $[E : E']$. Из приведенных выше рассуждений имеем:

$$[E_k(\xi) : F] = [E_k : E_{k'}]. \tag{3}$$

Расширение поля F элементами из $E_{k''}$ обозначим F'. Отсюда получаем:

$$1 < \left[F' : F\right] \leq [E_{k''} : E_{k'}].$$

Из полученного неравенства и равенства (3) следует, что F не является максимальным подполем в $E_k(\xi)$. Полученное противоречие означает, что $E_{k'}$ — максимальное подполе в E_k.

Покажем теперь, что в случае

$$E_k \not\subseteq F \tag{4}$$

максимальное подполе F содержит дробь степени 1. Имеет место равенство:

$$E_{k'}(a) = E_k,$$

и существует неприводимый над $E_{k'}$ многочлен $\hat{f}(z)$, $\hat{f} \in E_{k'}[z]$, для которого a является корнем. Через q обозначим $\deg \hat{f}$.

Из максимальности подполя F и соотношения (4) следует, что множество A,

$$A = \left\{ \ a^i \ \mid \ i \in \{0, 1, \ldots, q-1\} \ \right\}$$

образует базис $E_k(\xi)$ как линейого пространства над F. Поэтому для некоторых μ_i, $\mu_i \in F$, $i = 0, 1, \ldots, q-1$, имеет место тождество:

$$\xi = \sum_{i=0}^{q-1} \mu_i a^i.$$

Пусть дроби $\mu_i = \frac{u_i}{v_i}$ представлены в несократимом виде, $i = 0, 1, \ldots, q-1$. Так как $\xi \notin E_k$, то найдется i_0, $i_0 \in \{i = 0, 1, \ldots, q-1\}$, такое, что $\deg \mu_{i_0} \geq 1$.

Многочлен $h_1(z)$, $h_1(z) = \mu_{i_0} v_{i_0}(z) - u_{i_0}(z)$, имеет корень $z = \xi$, поэтому он делится на $h_0(z)$, $h_0(z) = z - \sum_{i=0}^{q-1} \mu_i a^i$ в кольце $E_k(\xi)[z]$ без остатка, так как множество A линейно независимо над F. Таким образом, для некоторого многочлена $\tilde{f}$, $\tilde{f} \in E_k(\xi)[z]$, имеет место равенство:

$$h_1 = \tilde{f} h_0.$$

Можно показать, что $\tilde{f}$ не зависит от переменной ξ, поэтому многочлен $h_0(z) = h_1/\tilde{f}$ степени 1 по z имеет коэффициенты из $E_k(\mu_{i_0})$ и корень $z = \xi$. Таким образом,

$$E_k\left(\mu_{i_0}\right) = E_k(\xi),$$

откуда вытекает равенство:

$$F = E_{k'}\left(\mu_{i_0}\right).$$

При этом, $\deg \mu_{i_0} = 1$. Не ограничивая общности, можно предположить, что $\mu_{i_0} \in E'_k(\xi)$.

Несложно показать, что для любого максимального подполя $E_{k'}$ поля E_k и любого μ, $\mu \in E'_k(\xi)$, $\deg \mu = 1$, найдется пара p, ω, для которой выполнено включение:

$$E_{k'} \cup \{\mu\} \subset M^{(1)}_{p,\omega}.$$

Из этого включения путем некоторых рассуждений получаем:

$$E_{k'}(\mu) \cap E'_k(\xi) \subseteq M^{(1)}_{p,\omega}.$$

Поэтому рассматриваемое множество M не может содержаться в $E_{k'}(\mu)$.

Лемма 1 доказана.

Введем следующие подмножества $E'_k(\xi)$.

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

$$\tilde{R}^{(1)}_p = \left\{ \ \mu \ \mid \ \mu \in E'_k(\xi), \ \ \mu = \frac{u}{v}, \ \ (v,p) = 1 \ \right\},$$

$p \in I_k$.

Лемма 2. *Пусть множество дробей M из $E'_k(\xi)$ не содержится ни в одном классе множества $J^{(1)}_k$. Тогда для любого ρ, $\rho \in I_k \cup \{0\}$, выполнено:*

$$K^{(1)}(M) \not\subseteq \tilde{R}^{(1)}_\rho.$$

Доказательство леммы.

Пусть $M \subseteq E'_k(\xi)$,

$$\forall \Theta, \ \ \Theta \in J^{(1)}_k, \ \ M \not\subseteq \Theta. \tag{5}$$

Покажем, что для каждого ρ, $\rho \in I_k \cup \{0\}$, для которого

$$M \subseteq \tilde{R}^{(1)}_\rho, \tag{6}$$

в $K(M)$ содержится дробь μ'_ρ, удовлетворяющая соотношениям $\mu'_\rho(0) = 0$ и $\mu'_\rho \notin R^{(1)}_\rho$.

Пусть для некоторого ρ выполнено (6). Из соотношений (5) для $\Theta \in \{ \ P_\Delta \ \mid \ \Delta \in W_k \ \}$ вытекает, что в $K^1(M)$ содержится дробь μ такая, что $\mu(0)$ является примитивным элементом поля E_k.

Через $\tilde{\mu}$ обозначим элемент множества $M \setminus R^{(1)}_\rho$. Если дробь $\tilde{\mu}$ не является искомой, то $\tilde{\mu}(0) \neq 0$. поэтому для некоторой степени $\tilde{s}$ имеем: $\tilde{\mu}(0) = \mu^{\tilde{s}}(0)$. Если при этом $\mu \in R^{(1)}_\rho$, то $\tilde{\mu} - \mu^{\tilde{s}}$ — искомый элемент $K^1(M)$.

Рассмотрим случай $\mu \notin R^{(1)}_\rho$. Если для любого ω, $\omega \in \Omega$, $\mu \notin M^{(1)}_{\rho,\omega}$, то через f обозначим ненулевой многочлен минимальной степени из $E_p[z]$, имеющий корень $\mu(0)$. Нетрудно видеть, что $f(\mu)$ — искомый.

Осталось рассмотреть случай $\mu \in M^{(1)}_{\rho,\omega}$ для некоторого ω, $\omega \in \Omega$. В M, в соответствии с (5) найдется дробь $\hat{\mu}$, $\hat{\mu} \notin M^{(1)}_{\rho,\omega}$. Если $\hat{\mu}(0) = 0$, то $\hat{\mu}$ — искомая. В противном случае, найдется $\hat{s}$, что $\hat{\mu} - \mu^{\hat{s}}$ — искомая.

Требуемое свойство множества M доказано. Утверждение леммы следует теперь из лемм 6 и 7 работы [6].

Лемма доказана.

Доказательство теоремы. Замкнутость классов из множества $J^{(1)}_k$ проверяется с использованием определений этих классов.

Если множество M не содержится ни в одном классе из $J^{(1)}_k$, то по лемме 1, с учетом расширяемости каждого множества из $E_k(\xi)$, не порождающего все $E_k(\xi)$, до максимального подполя, получаем равенство:

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

Отсюда, из теоремы 3 работы [6] и леммы 2 следует равенство

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

Таким образом, $J^{(1)}_k$ является критериальной системой.

Приведенность множества $J^{(1)}_k$, то есть не включение никакого класса Θ этого множества в любой его другой класс Θ' проверяется предъявлением элемента из $\Theta \setminus \Theta'$.

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] Кудрявцев В.Б., Алешин С.В., Подколзин А.С., *Введение в теорию автоматов*, «Наука», Москва, 1985, 320 с.

[4] Ленг С., *Алгебра*, пер. с англ., «Мир», Москва, 1968, 564 с.

[5] Лидл Р., Нидеррайтер Г., *Конечные поля*, пер. с англ., «Мир», Москва, 1988, 430 с.

[6] Часовских А.А., “Проблема полноты для класса линейно-автоматных функций”, *Дискретная математика*, **27**:2 (2015), 134–51

[7] Часовских А.А., “Условия полноты линейно-р-автоматных функций”, *Интеллектуальные системы*, **18**:3 (2014), 203–252

[8] Часовских А.А., “Приведенные критериальные системы предполных классов в классах линейных автоматов над конечными полями”, *Интеллектуальные системы*, **22**:4 (2018), 115–134

On classes of transfer functions of linear automata

Chasovskikh A.A.

For classes of transfer functions of linear automata over a finite field with operations induced by composition operations on these automata, all maximal subclasses are found.

Keywords: finite automaton, linear automaton, transfer function, operation of composition, feedback, completeness, closed class, maximum subclass, finite field.