Задача К-конечнопорожденности для предполных классов линейных автоматов, составляющих А-критериальную систему в пространстве линейных автоматов.

В. А. Бирюкова[1]

В данной статье рассматривается проблема К- и А-конечнопорожденности для предполных классов линейных автоматов, функционирующих над полем Галуа, состоящим из двух элементов. Для каждого исследуемого класса был предъявлен конечный базис. Совокупность исследуемых классов составляет А-критериальную систему в классе линейных автоматов.

Ключевые слова: конечный автомат, линейный автомат, операции композиции, обратная связь, полнота, замкнутый класс, предполный класс, К-конечнопорожденный класс, А-конечнопорожденный класс.

1. Введение

С середины прошлого века вплоть до настоящего времени не уменьшается интерес к изучению различных свойств конечных автоматов. Конечный автомат можно представить как устройство, в каждый дискретный момент времени пребывающее в одном из конечного числа состояний и обладающее входом и выходом [1]. Описать действие автомата можно с помощью функций k-значной логики. Труды по данной тематике принадлежат таким видным ученым как С.К. Клини [2], Э.Ф. Муру [3], Дж. фон-Нейману [4] и др. В рамках отечественной школы кибернетики начало положили такие известные ученые, как С.В. Яблонский [5], О.Б. Лупанов [6] и В.Б. Кудрявцев [7],[8].

Интересной задачей является изучение вопросов, рассмотренных как для всего пространства конечных автоматов, так и для его различных подмножеств. В частности, задачи полноты и конечнопорожденности для подклассов конечных автоматов, изучение структуры данных подклассов - например, какие предполные или замкнутые классы есть и т.п.

[1] *Бирюкова Вероника Андреевна* — аспирант кафедры Математической теории интеллектуальных систем механико-математического факультета МГУ, e-mail: biryukovaveronika@mail.ru.

Biryukova Veronika Andreevna — graduate student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

В работах А.А. Часовских [9]-[12] подробно рассматриваются вопросы полноты и выразимости в классе линейных автоматов над произвольными конечными полями. Проблема линейной реализуемости автоматов — представления линейными функциями автоматов, функционирующих над конечными полями, — излагается, в частности, в книге А. Гилла "Линейные последовательностные машины"[13].

Естественным продолжением работ в этом направлении является изучение вопросов конечнопорожденности относительно разных множеств операций для различных классов линейных автоматов. В представленной работе будут решены задачи К- и А- конечнопорожденности для предполных классов линейных автоматов, совокупность которых представляет собой А-критериальную систему в пространстве линейных автоматов.

2. Основные понятия

С помощью шестерки $V = (A, Q, B, \varphi, \psi, q_0)$ можно задать инициальный абстрактный конечный автомат [1].Обозначим поле Галуа, состоящее из k элементов E_k. Если существуют натуральные числа $n, s \in \mathbb{N}$ такие, что $A = E_k^n,\ Q = E_k^s,\ B = E_k$ и φ, ψ являются линейными операторами k-значной логики, то автомат V является линейным автоматом.

В данной работе рассматриваются линейные автоматы над полем E_2. Мы будем применять к автоматам операции композиции, определенные в соответствии с работой [1]. Равными автоматами мы называем автоматы, задающие на существенных переменных равные ограниченно-детерминированные функции и отличающиеся только множеством (возможно пустым) фиктивных переменных.

Таким образом, мы будем рассматривать операции переименования переменных, отождествления переменных, подстановки одного автомата на вход другого автомата и операции обратной связи [1] как операции композиции.

Через $\mathcal{B}$ обозначим множество автоматов, состоящее из сумматора по модулю два, инвертора и задержки с нулевым начальным состоянием.

Линейные автоматы над E_2 получаем из множества $\mathcal{B}$, используя замыкание по операциям композиции.

Обозначим L_2 множество всех линейных автоматов над полем E_2.

Пусть $M \subseteq L_2$ — некоторое подмножество линейных автоматов. Будем называть K-замыканием $K(M)$ множество всех линейных автоматов, полученных с помощью операций композиции из элементов множества M.

Если $M \subseteq L_2,\ K(M) = M$, то M является K-замкнутым классом.

Если $M \subseteq L_2,\ K(M) = L_2$, то M является K-полным множеством.

Если $M \subset L_2,\ M \neq L_2,\ K(M) = M,\ \forall\, f \in L_2 \backslash M,\ K(\{f\} \cup M) = L_2$, то M есть K-предполный класс.

K-замкнутый класс M называется K-конечнопорожденным, если $\exists\, \{f_1, \ldots, f_m\} \subseteq M:\ M = K(\{f_1, \ldots, f_m\})$.

Также можно рассмотреть в пространстве L_2 оператор A-замыкания — аппроксимационного замыкания. Для этого введем несколько вспомогательных определений.

Пусть $f(x_1, \ldots, x_n) \in L_2,\ M \subseteq L_2,\ \tau \in \mathbb{Z}_+$.

Если существует $g(x_1, \ldots, x_n) \in K(M)$ такой, что для любых входных последовательностей $\alpha_i = a_i(0)a_i(1)\ldots,\quad i = \overline{1, n}$ автоматы f и g будут выдавать последовательности, совпадающие на первых τ элементах (обозначим подобное свойство так: $f(\alpha_1, \ldots, \alpha_n) \stackrel{\tau}{=} g(\alpha_1, \ldots, \alpha_n),$) то говорим, что f — τ-выразима через M.

Если f — τ-выразима через M для любого $\tau \in \mathbb{Z}_+$, то f — выразима через M.

Определим понятие оператора аппроксимационного замыкания множества M. Оператор A-замыкания сопоставляет множеству автоматов M множество всех автоматов, выразимым через M, т.е. $A(M) = \Big\{ f \ \Big|\ f \in L_2,\ f \text{ — выразим через } M\ \Big\}$.

Аналогично оператору K-замыкания для аппроксимационного замыкания вводятся понятия замкнутости, полноты, предполноты и конечнопорожденности.

Если $A(M) = M$, то M является A-замкнутым классом.

Если $A(M) = L_2$, то M есть A-полное множество.

Если $M \subset L_2,\ M \neq L_2,\ K(M) = M,\ \forall\, f \in L_2 \backslash M,\ A(\{f\} \cup M) = L_2$, то M — A-предполный класс.

A-замкнутый класс M называется A-конечнопорожденным, если $\exists\, \{f_1, \ldots, f_m\} \subseteq M : M = A(\{f_1, \ldots, f_m\})$.

Введем для формальных степенных рядов над полем E_2 следующее обозначение:

$R_2(\xi) = \left\{ \sum\limits_{t=0}^{\infty} a(t)\xi^t \ \mid a(0), \ldots, a(t), \ldots \in E_2^{\infty} \right\}$ – множество формальных степенных рядов переменной ξ с коэффициентами из поля E_2.

$E_2^{\infty} = \Big\{ a(0), \ldots, a(t), \ldots \mid\, t \in \mathbb{N}, \forall\ t\ a(t) \in E_2 \Big\}$ — это множество бесконечных последовательностей элементов поля E_2.

$E_2'(\xi) = \left\{ \sum\limits_{t=0}^{\infty} a(t)\xi^t \ \mid a(0), \ldots, a(t), \ldots \in E_2^{\infty} \text{— периодическая (с предпериодом) последовательность} \right\} \subset R_2(\xi).$

Также для $E_2'(\xi)$ есть эквивалентное определение [9] через многочлены от переменной ξ:

$E_2'(\xi) = \left\{ \frac{u}{v} \mid u, v \in E_2[\xi], \ v = 1 + \xi \cdot v', v' \in E_2[\xi] \right\} = \left\{ \frac{u}{v} \mid u, v \in E_2[\xi], \ v(0) = 1 \right\}.$

Таким образом, $E_2'(\xi)$ является подкольцом поля отношений $E_2(\xi)$ [14].

Автомат f можно рассматривать как преобразователь формальных рядов:

$$f(x_1, \ldots, x_n) : (R(\xi)_2)^n \to R_2(\xi), \tag{3}$$

где x_i принимают значения из $R_2(\xi)$ $\forall\, i = \overline{1, n}$.

В работе [9] доказано, что любой линейный автомат может быть представлен следующим образом:

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0, \tag{4}$$

где $n \in \mathbb{N}$, $\mu_j \in E_2'(\xi)\ \forall\, j = \overline{0, n}$, x_i принимают значения из $R_2(\xi)$ $\forall\, i = \overline{1, n}$.

И наоборот, любой автомат $f(x_1, \ldots, x_n)$, представимый в виде (4), является линейным.

Введем обозначение для множества коэффициентов μ_i при переменных автомата f: $U(f) = \{\mu_1, \ldots, \mu_n\}$.

Не трудно заметить, что переменная x_i является существенной переменной линейного автомата f, если $\mu_i \neq 0$. Переменная x_i называется непосредственной переменной линейного автомата f, если $\mu_i(0) = 1$.

Пусть линейный автомат f задан равенством (4). Рассмотрим, как применение операций композиции выражается в терминах представления (4).

1) Переименование переменных.

$$f(x_1, \ldots, x_{n-1}, x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0 = \sum_{i=1}^{n} \mu_i \tilde{x}_i + \mu_0 = f(\tilde{x}_1, \ldots, \tilde{x}_{n-1}, \tilde{x}_n). \tag{5}$$

2) Отождествление переменных. Без ограничения общности пусть у линейного автомата $f(x_1,\ldots,x_n)$ отождествлены переменные x_{n-1} и x_n. Тогда

$$f(x_1,\ldots,x_{n-1},x_{n-1}) = g(x_1,\ldots,x_{n-1}) = \sum_{i=1}^{n-2}\mu_i x_i + \big(\mu_{n-1}+\mu_n\big)x_{n-1}+\mu_0. \tag{6}$$

Таким образом, отождествление переменных x_{n-1} и x_n линейного автомата f приводит к сложению коэффициентов μ_{n-1} и μ_n.

3) Подстановка одного автомата на вход другого автомата. Пусть есть линейные автоматы $f(x_1,\ldots,x_n)$ и $h(x'_1,\ldots,x'_m)$. Без ограничения общности пусть автомат h подставляется на n-ый вход автомата f. Тогда:

$$f(x_1,\ldots,x_n) = \sum_{i=1}^{n}\mu_i x_i + \mu_0, \tag{7}$$

$$h(x'_1,\ldots,x'_m) = \sum_{i=1}^{m}\mu'_i x'_i + \mu'_0, \tag{8}$$

$$g(x_1,\ldots,x_{n-1},x'_1,\ldots,x'_m) = f(x_1,\ldots,x_{n-1},h(x'_1,\ldots,x'_m)), \tag{9}$$

$$g(x_1,\ldots,x_{n-1},x'_1,\ldots,x'_m) = \sum_{i=1}^{n-1}\mu_i x_i + \mu_0 + \mu_n\cdot\left(\sum_{i=1}^{m}\mu'_i x'_i + \mu'_0\right) =$$

$$= \sum_{i=1}^{n-1}\mu_i x_i + \sum_{i=1}^{m}\mu_n\mu'_i x'_i + (\mu_n\mu'_0+\mu_0). \tag{10}$$

Как видно из выражения (10), операция подстановки линейного автомата h на n-ый вход автомата f приводит к умножению коэффициентов автомата h на коэффициент μ_n автомата f.

4) Обратная связь. Пусть дан линейный автомат $f(x_1,\ldots,x_n)$, и к переменной x_n может быть применена операция обратной связи, т.е. значение автомата f в момент времени t не зависит от $x_n(t)$. Замечу, что в терминах представления (4) к переменной x_n может быть применена операция обратной связи $\Leftrightarrow$ $\mu_n(0)=0$. Тогда [9]:

$$Fb_{x_n}\big(f(x_1,\ldots,x_n)\big) = g(x_1,\ldots,x_{n-1}) = \frac{1}{1+\mu_n}\left(\sum_{i=1}^{n-1}\mu_i x_i + \mu_0\right) =$$

$$= \sum_{i=1}^{n-1} \frac{\mu_i}{1+\mu_n} \cdot x_i + \frac{\mu_0}{1+\mu_n}. \qquad (11)$$

Таким образом, применение операции обратной связи к линейному автомату f по переменной x_n приводит к применению на коэффициентах автомата f операции Fb, определенной на элементах класса $E_2'(\xi)$ далее.

Операции композиции над линейными автоматами индуцируют следующие операции над элементами μ_1 и μ_2, $\mu_1, \mu_2 \in E_2'(\xi)$:

1. Операция сложения элементов μ_1 и μ_2 : $\mu_1 + \mu_2$.

2. Операция умножения элементов μ_1, μ_2 : $\mu_1 \cdot \mu_2$.

3. Операция обратной связи, примененная к элементам μ_1 и μ_2 при условии, что $\mu_2(0) = 0 : Fb(\mu_1, \mu_2) = \frac{\mu_1}{1+\mu_2}$.

Также $E_2'(\xi)$ можно считать множеством одноместных линейных автоматов, сохраняющих нулевую последовательность, к которым можно применять операции 1-3. Таким образом, на $E_2'(\xi)$ вводится оператор $K^{(1)}$-замыкания. Аналогично введем и другие понятия:

M есть $K^{(1)}$-замкнутый класс $\Leftrightarrow$ $M \subseteq E_2'(\xi)$, $K^{(1)}(M) = M$.

M называется $K^{(1)}$-полным множеством $\Leftrightarrow M \subseteq E_2'(\xi)$, $K^{(1)}(M) = E_2'(\xi)$.

Если $M \subset E_2'(\xi)$, $M \neq E_2'(\xi)$, $K^{(1)}(M) = M, \forall\ \mu \in E_2'(\xi) \backslash M \quad K^{(1)} (M \cup \{\mu\}) = E_2'(\xi)$, то M является $K^{(1)}$-предполным классом.

$K^{(1)}$-замкнутый класс M называется $K^{(1)}$-конечнопорожденным, если $\exists\ \{\mu_1, \ldots, \mu_m\} \subseteq M : M = K^{(1)}(\{\mu_1, \ldots, \mu_m\})$.

Пронумеруем неприводимые многочлены над E_2: $p_1 = \xi$, $p_2 = 1 + \xi$, $p_3 = 1 + \xi + \xi^2, \ldots$

В работе [9] были найдены все $K^{(1)}$-предполные классы, совокупность которых образует $K^{(1)}$-критериальную систему в $E_2'(\xi)$, т.е. $M \subseteq E_2'(\xi)$ будет $K^{(1)}$-полным множеством тогда, и только тогда, когда M не принадлежит ни одному классу этой системы.

В

$M_i^{(1)} = \big\{\mu \mid \mu \in E_2'(\xi),\ \mu + \mu(0) = \xi \cdot p_i \cdot \mu',\ \mu' = \frac{u'}{v'} \in E_2'(\xi),\ (v', p_i) = 1\big\}$, $i \in \mathbb{N}$.

Рассмотрим следующие подмножества автоматов в L_2.

$T_0 = \big\{f \big| \ f \in L_2,\ \mu_0(0) = 0\big\}$,

$T_1 = \big\{f \big| \ f \in L_2,\ \sum\limits_{i=0}^{n} \mu_i(0) = 1\big\}$,

$V_1 = \{f \mid f \in L_2,\ f$ имеет не более 1 непосредственной переменной$\}$,

$V_2 = \{f \mid f \in L_2,\ f$ имеет нечетное число непосредственных переменных$\}$,

$M_1 = \{f \mid f \in L_2, \forall\, \mu \in U(f), \mu \in M_1^{(1)}\}$.

Для данных множеств линейных автоматов имеет место следующая теорема:

Теорема [9].

$$M \subseteq L_2,\ A(M) = L_2 \Leftrightarrow M \not\subseteq \theta,\ \forall\, \theta \in \mathcal{J}_A = \{T_0, T_1, V_1, V_2, M_1\}. \tag{12}$$

То есть система классов $\mathcal{J}_A$ является A-критериальной системов в L_2.

3. K-конечнопорожденность предполных классов из системы предполных классов J_A

Лемма 1. *K-предполный класс линейных автоматов T_0 порождается множеством $M = \{\xi \cdot x,\ x_1 + x_2,\ \xi\}$, которое является базисом данного класса.*

Доказательство. Рассматривается класс автоматов $T_0 = \{f \mid f \in L_2, \mu_0(0) = 0\}$. Автомат этого класса f в представлении (4) имеет следующий вид:

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0,\ \forall\, \mu_i \in E_2'(\xi),\ i = \overline{1,n},\ \mu_0 \in E_2'(\xi) : \mu_0(0) = 0. \tag{1}$$

Покажем, что $K(M) = T_0$. Обозначим элементы множества M: $f_1 = \xi \cdot x,\ f_2 = x_1 + x_2,\ f_3 = \xi$. Все три автомата принадлежат классу T_0, так как сохраняют ноль в начальный момент времени. Поскольку класс T_0 K-замкнут, то $K(M) \subset T_0$.

Нулевой автомат содержится в $K(M)$: $f_2(x,x) = x + x = 0 \in K(M)$.

Проводник принадлежит K-замыканию множества M: $f_2(x, 0) = x + 0 = x \in K(M)$.

Также верно, что $\forall\ m \in \mathbb{N}\quad \xi^m x \in K(M)$, т.к. можно $(m-1)$ раз подставить автомат f_1 в себя: $f_1(f_1(..(f_1(x)\ldots) = \xi^m x \in K(M)$.

И для любого многочлена $u = \sum_{i=0}^{s} a_i \xi^i \in E_2[\xi],\ s \in \mathbb{Z}_+,\ u \cdot x \in K(M):$

$$u \cdot x = \left(\sum_{i=0}^{s} a_i \xi^i\right) x = \sum_{i=0}^{s} a_i \xi^i x \in K(M). \tag{2}$$

Также можно показать, что для любого элемента $\mu \in E_2'(\xi)$ $\mu \cdot x \in K(M)$. Действительно, произвольный элемент $E_2'(\xi)$ можно представить с помощью многочленов: $\mu = \dfrac{u}{v}$, $u, v \in E_2[\xi]$, $v(0) = 1$, т.е. $v = 1 + \xi v'$, $v' \in E_2[\xi]$. Выше было доказано, что $\forall\, v' \in E_2[\xi]$ $\xi \cdot v' \cdot x \in K(M)$, поэтому, применив операцию обратной связи к автомату $f(x_1, x_2) = u \cdot x_1 + \xi \cdot v' \cdot x_2 \in K(M)$ по переменной x_2 (данная переменная не является непосредственной, вследствие чего эта операция применима по x_2), получим искомый автомат:

$$Fb_{x_2}(f(x_1, x_2)) = \frac{u \cdot x_1}{1 + \xi \cdot v} = \mu \cdot x \in K(M). \tag{3}$$

Заметим, $f \in T_0 \Leftrightarrow \mu_0(0) = 0$. То есть свободный член автомата из класса T_0 можно представить так: $\mu_0 = \xi \cdot \mu'$, $\mu' \in E_2'(\xi)$. Для любого $\mu' \in E_2'(\xi)$ $f(x) = \mu' \cdot x \in K(M)$, поэтому, подставив в f автомат $f_3 \in M$, получим любую константу из T_0. Используя сумматор, можно получить любой автомат из T_0. Таким образом, $T_0 \subset K(M)$, благодаря чему $K(M) = T_0$.

Множество М является базисом класса T_0. Задержку исключить нельзя, т.к. в K-замыкании сумматора и ξ можно получить только функции вида $f(x_1, \ldots, x_n) = x_1 + + \ldots + x_n + a_0\xi$, $a_0 \in E_2$, т.е. $\xi x \notin K(\{x_1 + x_2, \xi\})$. Без сумматора не получим автомата более, чем от одной переменной, что не есть весь класс $T_0 : K(M \backslash \{x_1 + x_2\}) \neq T_0$. Заметим, что сумматор и задержка сохраняют последовательность длины 2 $C = 00$, а ξ её не сохраняет (данный автомат выдает последовательность $\tilde{C} = 01$), поэтому ξ нельзя исключить из порождающей класс T_0 системы автоматов M. Можно показать, $\xi \notin K(\{f_1, f_2\})$. В связи с чем приходим к выводу, что множество M является базисом класса T_0. Лемма полностью доказана.

$\square$

Лемма 2. *K-предполный класс линейных автоматов T_1 порождается множеством $M = \{f_1, f_2, f_3\} = \{x_1 + x_2 + x_3,\ \ \xi \cdot x + 1,\ 1\}$, которое является базисом данного класса.*

Доказательство. Класс T_1 есть класс автоматов, сохраняющих единицу в начальный момент времени. В представлении (4) это свойство можно выразить так:

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0 \ \in T_1 \Leftrightarrow \sum_{j=0}^{n} \mu_j(0) = 1. \tag{4}$$

Покажем, что $K(M) = T_1$. Каждый автомат из M сохраняет единицу в начальный момент, т.е. принадлежат классу T_1. В силу K-замкнутости класса T_1, $K(M) \subset T_1$.

Проводник можно получить в K-замыкании множества M, отождествив переменные автомата $f_1 : f_1(x, x, x) = x + x + x = x \in K(M)$.

Для любого натурального m получим автомат вида $(\xi^m + 1) \cdot x$. Для этого сначала подставим $(m - 1)$ раз автомат f_2 в себя:

$$\tilde{f}_m(x) = \xi(\xi(\ldots\xi(\xi x + 1) + 1)\ldots) + 1 =$$

$$= \xi^m \cdot x + (\xi^{m-1} + \xi^{m-2} + \ldots + \xi + 1) \in K(M). \tag{5}$$

Далее, подставляя f_3 в автоматы $\tilde{f}_m(x)$, можно получить для любого m все константы вида $c_m = (\xi^m + \xi^{m-1} + \xi^{m-2} + \ldots + \xi + 1) \in K(M)$. Тогда сделаем следующее:

$$f_1(\tilde{f}_m(x), c_{m-1}, x) = \big(\xi^m \cdot x + (\xi^{m-1} + \xi^{m-2} + \ldots + \xi + 1)\big) +$$

$$+ (\xi^{m-1} + \xi^{m-2} + \ldots + \xi + 1) + x = (\xi^m + 1) \cdot x \in K(M). \tag{6}$$

Покажем, что для любого многочлена $\tilde{u} \in E_2[\xi]$ в K-замыкании множества M есть автомат $(1 + \xi\tilde{u}) \cdot x \in K(M)$. Пусть $\tilde{u} = a_1 + a_2\xi + \ldots + a_s\xi^{s-1} + a_{s+1}\xi^s,\ s \in \mathbb{N}$. Также введем многочлен u:

$$u = 1 + \xi\tilde{u} = 1 + \xi(a_1 + a_2\xi + \ldots + a_s\xi^{s-1} + a_{s+1}\xi^s) =$$

$$= 1 + a_1\xi + a_2\xi^2 + \ldots + a_s\xi^s + a_{s+1}\xi^{s+1}. \tag{7}$$

Как было показано выше, для любого натурального m, в том числе и для $m : m = \overline{1, (s + 1)},\ g_m(x) = (a_m\xi^m + 1) \cdot x \in K(M)$ (если $a_m = 0$, то соответствующий член многочлена является проводником, который также есть в $K(M)$).

Рассмотрим 2 случая:

1) s - четное число. Тогда слагаемых в $\tilde{u}$ $(s + 1)$ нечетное количество. В таком случае, в сумматор от $s+1$ переменной f_{s+1} (подставляя автомат f_1 в себя, в $K(M)$ можно получить сумматор от любого нечетного числа переменных) подставляются автоматы $g_m(x),\ m = \overline{1, (s + 1)}$:

$$f_{s+1}(g_1(x), \ldots, g_{s+1}(x)) = \sum_{m=1}^{s+1}(a_m\xi^m + 1) \cdot x = \sum_{m=1}^{s+1} a_m\xi^m \cdot x + x =$$

$$= (1+a_1\xi+\ldots+a_{s+1}\xi^{s+1})x = (1+\xi(a_1+\ldots+a_{s+1}\xi^s))x = (1+\xi\tilde{u})x \in K(M). \tag{8}$$

2) s - нечетное число, т.е. в $\tilde{u}$ $(s+1)$ слагаемых четное количество. Тогда в сумматор от $s+2$ переменных f_{s+2} подставляются автоматы $g_m(x),\ m=\overline{1,(s+1)}$ и проводник:

$$f_{s+2}(g_1(x),\ldots,g_{s+1}(x),x)=\sum_{m=1}^{s+1}(a_m\xi^m+1)\cdot x+x=$$

$$=\sum_{m=1}^{s+1}a_m\xi^m\cdot x+x=(1+\xi\tilde{u})x\in K(M). \tag{9}$$

Также для любого $\mu\in E_2'(\xi)$ верно, что $(1+\xi\mu)\cdot x\in K(M)$. Представим μ в виде формальной дроби:

$$\mu=\frac{u}{1+\xi\cdot v},\ \ u,v\in E_2[\xi]. \tag{10}$$

Знаем, что $\forall\ u',v\in E_2[\xi]\quad(1+\xi u')x,\ (1+\xi v)x\in K(M)$ $(u=u'+v,u'=u+v)$. Подставим эти автоматы в f_1 и отождествим две переменные:

$$f_1((1+\xi u')x,(1+\xi v)x_1,x_1)=(1+\xi u')x+(1+\xi v)x_1+x_1=$$

$$=(1+\xi u')x+\xi vx_1\in K(M). \tag{11}$$

Затем применим операцию обратной связи по x_1 (переменная x_1 не является непосредственной, поэтому операция обратной связи применима по данной переменной):

$$Fb_{x_1}(f_1((1+\xi u')x,(1+\xi v)x_1,x_1))=\frac{1+\xi u'}{1+\xi v}x=$$

$$=\left(1+\xi\cdot\frac{u'+v}{1+\xi v}\right)x=(1+\xi\mu)x\in K(M). \tag{12}$$

Подставив в $(1+\xi\mu)x$ автомат f_3, получим в $K(M)$ любую константу вида $(1+\xi\mu)$.

Введем ещё 2 вспомогательные функции из $K(M)$:

$$h_1(x,x_1)=f_1((1+\xi\mu)x,x,x_1)=(1+\xi\mu)x+x+x_1=\xi\mu x+x_1\in K(M) \tag{13}$$

$$h_2(x_1)=h_1(1,x_1)=\xi\mu+x_1\in K(M) \tag{14}$$

Для автомата из T_1 верно, что среди $n+1$ слагаемых его разложения (n переменных и 1 константа) нечетное число s слагаемых имеет вид (1): или $(1+\xi\mu)x$, или $(1+\xi\mu)$; остальные m слагаемых имеют вид (2): $\xi\mu x$ или $\xi\mu$.

Можно выделить 4 случая построения произвольного автомата из T_1.

1) n — четное число и свободный член автомата имеет вид (1). Тогда $s-1$ переменная имеет вид (1), оставшиеся $n-(s-1)=m$ (четное число) переменных имеют вид (2). В сумматор от $(n+1)$ переменной подставляются s автоматов вида (1) (они есть в $K(M)$), в оставшиеся позиции подставляются автоматы $h_1(x, x_1)$, при этом переменная x_1 отождествляется и, ввиду четности m, сокращается.

2) n — четное число и свободный член автомата имеет вид (2). Тогда s переменных имеет вид (1), оставшиеся $n-s=m-1$ (нечетное число) переменных имеют вид (2). В сумматор от $(n+1)$ переменной подставляются s автоматов вида (1) (они есть в $K(M)$), в оставшиеся позиции подставляются автоматы $h_1(x, x_1)$, $h_2(x_1)$, при этом в полученном автомате переменная x_1, ввиду четности m, сокращается.

3) n — нечетное число и свободный член автомата имеет вид (1). Тогда $s-1$ переменных имеет вид (1), оставшиеся $n-(s-1)=m$ (нечетное число) переменных имеют вид (2). В сумматор от $(n+2)$ переменной подставляются s автоматов вида (1) (они есть в $K(M)$), в оставшиеся позиции подставляются автоматы $h_1(x, x_1)$ и автомат $g(x_1)=x_1$, при этом переменная x_1 отождествляется, и, ввиду четности $(m+1)$, сокращается.

4) n — нечетное число и свободный член автомата имеет вид (2). Тогда s переменных имеет вид (1), оставшиеся $n-s=m-1$ (четное число) переменных имеют вид (2). В сумматор от $(n+2)$ переменной подставляются s автоматов вида (1) (они есть в $K(M)$), в оставшиеся позиции подставляются автоматы $h_1(x, x_1)$, $h_2(x_1)$ и автомат $g(x_1)=x_1$, при этом, ввиду четности m, переменная x_1 сокращается.

Подобным образом может быть получен любой автомат из класса T_1. Следовательно, $T_1 \subset K(M)$. Что приводит нас к заключению, что $T_1 = K(M)$.

Покажем, что множество M является базисом класса T_1. Сумматор $x_1+x_2+x_3$ является единственным автоматом в M от более, чем от одной переменной, поэтому $K(\{\xi \cdot x+1,\ 1\}) \neq T_1$. Без автомата $f_2 = \xi \cdot x + 1$ с помощью операций композиции из множества M можно получить только автоматы вида $f(x_1, \ldots, x_n) = x_1 + \ldots + x_n + a_0\xi$, $a_0 \in E_2$, т.е. $K(\{f_1, f_3\}) \neq T_1$. Заметим, что сумматор от трех переменных сохраняет любую последовательность произвольной длины. Автомат f_3 не содержится в K-замыкании $\{x_1+x_2+x_3,\ \xi \cdot x+1\}$, т.к. автоматы f_1, f_2 сохраняют последовательность длины 2: $C=11$, а f_3 выдает последовательность 10. Можно показать, что автомата f_3 в K-замыкании множества $\{f_1, f_2\}$ нет. В связи с чем, множество M является базисом класса T_1. Лемма доказана полностью.

$\square$

Лемма 3. *K-предполный класс линейных автоматов V_1 порождается множеством $M = \{f_1, f_2, f_3\} = \{\xi x_1 + x_2,\ \ \xi \cdot x,\ x+1\}$, которое является базисом данного класса.*

Доказательство. Автомат класса $V_1 = \Big\{ f \Big| \ f \in L_2,\ f$ имеет не более 1 непосредственной переменной $\Big\}$ в разложении (4) представляется в таком виде: $f(x_1, \ldots, x_n) = \sum\limits_{i=1}^{n} \mu_i x_i + \mu_0 \ \in V_1$.

x_i — непосредственная переменная автомата $f \Leftrightarrow \mu_i(0) = 1 \Leftrightarrow \mu_i = 1 + \xi\mu',\ \mu' \in E_2'(\xi)$.

Докажем, что $K(M) = V_1$. Каждый автомат множества M имеет не более 1 непосредственной переменной, и, поскольку класс V_1 является K-замкнутым, $K(M) \subset V_1$.

Нулевой автомат содержится в $K(M) : Fb_x(\xi x) = 0 \in K(M)$.

Проводник также есть в $K(M) : f_1(0, x) = x = 1 \cdot x \in K(M)$.

Подставив автомат f_2 в себя $m-1$ раз (для любого натурального m), получим автомат $\xi^m x \in K(M)$:

$$f_2(f_2(..(f_2(x)\ldots) = \xi^m x \in K(M). \tag{15}$$

Покажем, что для любого многочлена $u = \sum\limits_{i=0}^{s} = a_i \xi^i \in E_2[\xi],\ s \in \mathbb{Z}_+,\ u \cdot x \in K(M)$. Докажем этот факт для произвольного многочлена u с помощью математической индукции по степени многочлена s. Действительно, многочлены нулевой степени ($u = 0$, $u = 1$) реализуется в $K(M)$ с помощью нулевого автомата и проводника, присутствующих в $K(M)$. Для $s = 1$ многочлену $u = \xi$ соответствует автомат f_2, а для многочлена $u = \xi + 1$ в замыкании $K(M)$ есть такой автомат: $f_1(x, x) = \xi \cdot x + x = (\xi + 1)x \in K(M)$.

Пусть данный факт доказан для многочленов степени s. Тогда для любого многочлена степени $(s+1)$ $u = a_0 + \ldots + a_s\xi^s + \xi^{s+1}$ получим искомый автомат следующим образом:

$$f_1(\xi^s x, (a_0 + \ldots + a_s\xi^s)x) = \xi(\xi^s x) + (a_0 + \ldots + a_s\xi^s)x =$$

$$= (a_0 + \ldots + a_s\xi^s + \xi^{s+1})x = u \cdot x \in K(M). \tag{16}$$

Также для любого $\mu \in E_2'(\xi)$ верно, что $\mu \cdot x \in K(M)$. Представим элемент $E_2'(\xi)$ в виде дроби многочленов:

$$\mu = \frac{u}{1 + \xi \cdot v} \in E_2'(\xi),\ u, v \in E_2[\xi]. \tag{17}$$

В автомат f_1 подставим автоматы $ux, vx \in K(M) : f_1(vx_1, ux_2) = \xi vx_1 + ux_2 \in K(M)$. И применим операцию обратной связи по не непосредственной переменной x_1:

$$Fb_{x_1}(f_1(vx_1, ux_2)) = \frac{u}{1+\xi v} \cdot x_2 = \mu \cdot x_2 \in K(M). \tag{18}$$

Подставим в автомат f_3 нулевой автомат: $f_3(0) = 1 \in K(M)$. Подставив, в свою очередь, единицу в автоматы $\mu \cdot x$, получим в K-замыкании множества M любую константу μ из $E_2'(\xi)$.

Так как любой элемент $E_2'(\xi)$ представим или в виде $\mu = \xi\mu'$, или в виде $\mu = 1 + \xi\mu'$, $\mu' \in E_2'(\xi)$, то автомат $x + \mu$ также можно получить в K-замыкании множества M.
В первом случае в автомат f_1 подставим константу $\mu' \in K(M)$:

$$f_1(\mu', x) = \xi\mu' + x \in K(M). \tag{19}$$

Во втором случае в автомат f_3 поставим только что полученный автомат $\xi\mu' + x$:

$$f_3(\xi\mu' + x) = \xi\mu' + x + 1 = x + (1 + \xi\mu') = x + \mu \in K(M). \tag{20}$$

Заметим,что любой автомат f из V_1 имеет следующий вид:

$$f(x_1, \ldots x_n) = \sum_{i=1}^{n-1} \xi\mu_i' x_i + \mu_n x_n + \mu_0, \text{ где } \mu_n, \mu_0, \mu_i' \text{ любые элементы } E_2'(\xi). \tag{21}$$

Покажем, что любой такой автомат есть в $K(M)$. Подставляя на второй вход автомата f_1 самого себя, получим: $f_1(x_1, f_1(x_2, \ldots f_1(x_{n-1}, x_n) \ldots) = = \sum\limits_{i=1}^{n-1} \xi x_i + x_n$. Далее поставим на первые $n-1$ входов автоматы $\mu_i' x_i \in K(M)$, а на n-ый вход подставляется автомат $\mu_n x_n + \mu_0 \in K(M)$. Таким образом, любой автомат из класса V_1 содержится в K-замыкании множества $M : V_1 \subset K(M)$. И в связи с вышеизложенным получаем, что $V_1 = K(M)$.

Множество M является базисом класса V_1. Автоматы f_1 и f_3 сохраняют в начальный момент функции $\{x, \bar{x}\}$, а автомат f_2 не сохраняет (в начальный момент у данного автомата тождественный ноль). Можно показать, что ввиду наличия у f_2 такого свойства $f_2 \notin K(\{f_1, f_3\})$. Так как автомат f_1 является единственным автоматом от более, чем одной переменной, то $K(\{f_2, f_3\}) \neq V_1$. Заметим, что автоматы f_1, f_2 также принадлежат классу автоматов T_0, а автомат f_3 нет. В силу K-замкнутости класса $T_0 : f_3 \notin K(\{f_1, f_2\})$. В результате приходим к выводу, что множество M — базис класса V_1. Лемма полностью доказана.

□

Лемма 4. *K-предполный класс линейных автоматов V_2 порождается множеством $M = \{f_1, f_2, f_3\} = \{x_1+x_2+x_3,\ \ \xi\cdot x_1+x_2,\ x+1\}$, которое является базисом данного класса.*

Доказательство. Рассматриваемый класс V_2 — это класс линейных автоматов, имеющих нечетное число непосредственных переменных. В разложении (4) это свойство можно выразить следующим образом:

$$f(x_1,\ldots,x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0 \ \in V_2 \Leftrightarrow \sum_{i=1}^{n} \mu_i(0) = 1. \tag{22}$$

Покажем, что $K(M) = V_2$. Автомат f_1 имеет 3 непосредственные переменные, автоматы f_2, f_3 — 1 непосредственную переменную. Так как класс V_2 K-замкнут, то $K(M) \subset V_2$.

Отождествив переменные автомата f_1, получим в K-замыкании множества M проводник: $f_1(x,x,x) = x+x+x = x \in K(M)$.

Также в $K(M)$ для любого натурального m есть автомат $(\xi^m+1)x$. Подставим $m-1$ раз автомат f_2 в себя и отождествим переменные результирующего автомата:

$$\hat{f}_m(x) = \xi(\xi(\ldots\xi(\xi x+x)+x)\ldots+x)+x = (\xi^m x+\xi^{m-1}x+\xi^{m-2}x+\ldots+\xi x+x) =$$
$$= (\xi^m+\xi^{m-1}+\xi^{m-2}+\ldots+\xi+1)x \in K(M). \tag{23}$$

Затем подставим две подобные автоматные функции в f_1 и аналогично отождествим все переменные:

$$\tilde{f}_m(x) = f_1(\hat{f}_m(x), \hat{f}_{m-1}(x), x) = (\xi^m+\xi^{m-1}+\xi^{m-2}+\ldots+\xi+1)x+$$
$$+(\xi^{m-1}+\xi^{m-2}+\ldots+\xi+1)x + x = (\xi^m+1)x \in K(M). \tag{24}$$

Для любого многочлена $\tilde{u} \in E_2[\xi]$ в $K(M)$ можно получить автомат вида $(1+\xi\tilde{u})x$. Обозначим $\tilde{u} = a_1 + a_2\xi + \ldots + a_s\xi^{s-1} + a_{s+1}\xi^s$, $s \in \mathbb{Z}_+$. Также введем многочлен u:

$$u = 1+\xi\tilde{u} = 1+\xi(a_1+a_2\xi+\ldots+a_s\xi^{s-1}+a_{s+1}\xi^s) =$$
$$= 1+a_1\xi+a_2\xi^2+\ldots+a_s\xi^s+a_{s+1}\xi^{s+1}. \tag{25}$$

Докажем это включение, используя метод математической индукции по степени многочлена s. Для многочленов нулевой степени:

$$\tilde{u} = 0 \Rightarrow (1+0\cdot\xi)x = x \in K(M); \tag{26}$$

$$\tilde{u} = 1 \Rightarrow (1+1\cdot\xi)x = f_2(x,x) = \xi x + x \in K(M). \tag{27}$$

Для многочленов первой степени верно: $\tilde{u} = a_1 + \xi \Rightarrow u = 1 + \xi(a_1 + \xi) = 1 + a_1\xi + \xi^2$. Подставим в автомат f_1 автоматы $\tilde{f}_2(x)$, $(1 + a_1\xi)x \in K(M)$:

$$f_1(\tilde{f}_2(x), (1 + a_1\xi)x, x) = (\xi^2 + 1)x + (1 + a_1\xi)x + x =$$

$$= (1 + a_1\xi + \xi^2)x = (1 + \xi(a_1 + \xi))x \in K(M). \qquad (28)$$

Пусть для многочленов $\tilde{u}$ степени s утверждение верно. Докажем его для любого многочлена $\tilde{u}$ степени $s+1$. В автомат f_1 подставим автомат $\tilde{f}_{s+2}(x) \in K(M)$ и автомат $(1 + a_1\xi + + \ldots + a_{s+1}\xi^{s+1})x = (1 + \xi(a_1 + \ldots + a_{s+1}\xi^s))x \in K(M)$ (по предположению индукции такой автомат в K-замыкании множества M есть):

$$f_1(\tilde{f}_{s+2}(x),\ (1 + a_1\xi + \ldots + a_{s+1}\xi^{s+1})x,\ x) = (\xi^{s+2} + 1)x + (1 +$$

$$+ a_1\xi + \ldots + a_{s+1}\xi^{s+1})x + x = (1 + a_1\xi + \ldots + a_{s+1}\xi^{s+1} + \xi^{s+2})x =$$

$$= (1 + \xi(a_1 + \ldots + a_{s+1}\xi^s + \xi^{s+1}))x \in K(M). \qquad (29)$$

Для любого $\mu \in E_2'(\xi)$ покажем, что $(1 + \xi\mu) \cdot x \in K(M)$. В виде формальной дроби μ представляется так:

$$\mu = \frac{u}{1 + \xi \cdot v}, \quad u, v \in E_2[\xi]. \qquad (30)$$

Подставим в сумматор от трех переменных автоматы $(1 + \xi u')x$, $(1 + +\xi v)x$ и $x \in K(M) \quad \forall\, u', v \in E_2[\xi] \quad (u = u' + v, u' = u + v)$ соответственно и отождествим вторую и третью переменные:

$$g(x_1, x_2) = f_1((1 + \xi u')x_1, (1 + \xi v)x_2, x_2) =$$

$$= (1 + \xi u')x_1 + (1 + \xi v)x_2 + x_2 = (1 + \xi u')x + \xi v x_2 \in K(M). \qquad (31)$$

Затем применяется операция обратной связи по не непосредственной переменной x_2:

$$Fb_{x_2}(g(x_1, x_2)) = \frac{1 + \xi u'}{1 + \xi v}x_1 = \left(1 + \xi \cdot \frac{u' + v}{1 + \xi v}\right)x_1 = (1 + \xi\mu)x_1 \in K(M). \qquad (32)$$

Далее покажем, что для любой константы μ' из $E_2'(\xi)$ автомат $\mu x + +\mu' \in K(M)$ $(\mu = 1 + \xi\hat{\mu},\ \hat{\mu} \in E_2'(\xi))$. Для этого сначала докажем это для любого $\mu' = \tilde{u}$, где $\tilde{u} \in E_2[\xi]$. Многочлены нулевой степени: $\mu x + 0 \in K(M)$, $\quad \mu x + 1 = f_3(\mu x) \in K(M)$. Для многочленов первой степени также рассмотрим два случая.

Первый случай: $\tilde{u} = \xi$. Здесь на первый вход автомата f_2 подставим автомат f_3, затем отождествим переменные и получим следующее:

$$f_2(f_3(x), x) = \xi(x+1) + x = (1+\xi)x + \xi \in K(M). \tag{33}$$

Искомый автомат получим с помощью автомата f_1:

$$f_1((1+\xi)x + \xi, (1+\xi)x, \mu x) = \mu x + \xi \in K(M) \tag{34}$$

Второй случай: $\tilde{u} = \xi + 1$. В автомат f_3 подставим автомат из случая 1:

$$f_3(\mu x + \xi) = \mu x + \xi + 1 \in K(M). \tag{35}$$

Заметим, что для любого натурального m автомат $\xi^m + \mu x \in K(M)$. Действительно, пусть это утверждение верно для $m-1$ (для $m = 1$ доказано выше). Тогда:

$$f_2(\xi^{m-1} + x, x) = \xi(\xi^{m-1} + x) + x = \xi^m + (1+\xi)x \in K(M) \tag{36}$$

$$\begin{gathered} \tilde{g}_m(x) = f_1(f_2(\xi^{m-1} + x, x), (1+\xi)x, \mu x) = \\ = \xi^m + (1+\xi)x + (1+\xi)x + \mu x = \xi^m + \mu x \in K(M). \end{gathered} \tag{37}$$

Пусть для любого многочлена $\tilde{u}$ степени $m-1$ доказано, что $\mu x + \tilde{u} \in K(M)$. Покажем, что для любого многочлена $u = a_0 + a_1 \cdot \xi + \ldots + a_{m-1} \cdot \xi^{m-1} + \xi^m$ это утверждение также верно. Для этого в автомат f_1 подставим автоматы из K-замыкания множества M $(\xi^m + \mu x)$, μx, $(a_0 + +a_1\xi + \ldots + a_{m-1}\xi^{m-1}) + \mu x$:

$$\begin{gathered} f_1\Big(\big((a_0 + a_1\xi + \ldots + a_{m-1}\xi^{m-1}) + \mu x\big), \big(\xi^m + \mu x\big), \mu x\Big) = (a_0 + \\ +a_1\xi + \ldots + a_{m-1}\xi^{m-1}) + \mu x + \big(\xi^m + \mu x\big) + \mu x = (a_0 + \\ + a_1\xi + \ldots + a_{m-1}\xi^{m-1} + \xi^m) + \mu x = \mu x + \tilde{u} \in K(M). \end{gathered} \tag{38}$$

Также можно получить, что $\forall\, \mu_0 = \dfrac{u}{1+\xi v} \in E_2'(\xi)$, $u, v \in E_2[\xi]$ $\mu_0 + \mu x \in K(M)$ $(\mu : \mu(0) = 1)$. Сначала введем вспомогательный автомат:

$$\begin{gathered} g(x_1, x_2) = f_1\big(u + (1+\xi v)\mu x_1, (1+\xi v)x_2, x_2\big) = u + (1+\xi v)\mu x_1 + \\ + (1+\xi v)x_2 + x_2 = u + (1+\xi v)\mu x_1 + \xi v x_2 \in K(M). \end{gathered} \tag{39}$$

А затем применим операцию обратной связи по не непосредственной переменной x_2:

$$Fb_{x_2}(g(x_1, x_2)) = \frac{u}{1+\xi v} + \frac{1+\xi v}{1+\xi v}\mu x_1 = \mu_0 + \mu x_1 \in K(M). \qquad (40)$$

И, наконец, докажем, что любой автомат из V_2 от любого количества переменных принадлежит $K(M)$. Действительно, все автоматы из V_2 от одной переменной в $K(M)$ есть. Автоматы V_2 от двух переменных имеют одну непосредственную переменную и одну не непосредственную:

$$f(x_1, x_2) = (1 + \xi\mu_1')x_1 + \xi\mu_2' x_2 + \mu_0 \in V_2 \qquad (41)$$

Таким автоматы содержатся в $K(M)$:

$$f_1((1 + \xi\mu_1')x_1 + \mu_0,\ (1 + \xi\mu_2')x_2,\ x_2) = f(x_1, x_2) \in V_2 \qquad (42)$$

Пусть любой автомат $\hat{f}(x_1, \ldots, x_n)$ из V_2 от n переменных принадлежит $K(M)$. Чтобы увеличить количество непосредственных переменных для сохранности нечетности их числа, необходимо добавить сразу 2 непосредственные переменные x_{n+1} и x_{n+2} :

$$\tilde{f}(x_1,\ \ldots,\ x_n,\ x_{n+1},\ x_{n+2}) = \hat{f}(x_1,\ \ldots,\ x_n)\ +\ (1\ +\ \xi\mu_{n+1}')x_{n+1} +$$
$$+\ (1\ +\ \xi\mu_{n+2}')x_{n+2} \in K(M). \qquad (43)$$

Чтобы увеличить количество не непосредственных переменных достаточно добавить одну x_{n+1} переменную:

$$\tilde{f}(x_1, \ldots, x_n, x_{n+1}) = \hat{f}(x_1, \ldots, x_n) + (1 + \xi\mu_{n+1})\, x_{n+1} +\ x_{n+1} =$$
$$= \hat{f}(x_1, \ldots, x_n) + \xi\mu_{n+1}\, x_{n+1} \in K(M). \qquad (44)$$

Таким образом, любой автомат из V_2 содержится в $K(M)$: $V_2 \subset K(M)$. Следовательно, с учетом вышеизложенного $K(M) = V_2$.

Докажем, что порождающая система M является базисом класса V_2. Действительно, автоматы $f_1, f_2 \in T_0$ — K-замкнутому классу, отличному от V_2, т.е. $K(\{f_1, f_2\}) \neq V_2$ (автомат $f_3 \notin T_0$). Исключить автомат f_2 не получится, поскольку в K-замыкании сумматора от трех переменных и автомата f_3 можно получить только автоматы вида $f(x_1, \ldots, x_{2m+1}) =$

$x_1 + \ldots + x_{2m+1} + a_0, \quad a_0 \in E_2$, т.е. $f_2 \notin K(\{f_1, f_3\})$. А без сумматора от трех переменных нельзя получить автомат, у которого будет n непосредственных переменных для любого нечетного числа n. Заметим, что среди операций композиции только операция подстановки позволяет увеличивать количество переменных автомата, но с помощью этой операции, в K-замыкании автоматов f_2, f_3 нельзя получить автомат более, чем от одной непосредственной переменной. На основании вышеизложенного приходим к выводу, что множество M является базисом класса V_2. Лемма доказана полностью.

□

Лемма 5. *K-предполный класс линейных автоматов M_1 порождается множеством $M = \{f_1, f_2, f_3, f_4\} = \{\xi^3 x_1 + x_2 + x_3,\ \ \xi^2 \cdot x,\ 1,\ \xi\}$, которое является базисом данного класса.*

Доказательство. По определению класса M_1 любой коэффициент $\mu \in U(f)$ при переменной принадлежит классу $M_1^{(1)}$. В разложении (4) любой автомат класса M_{1n} представляется так:

$$f(x_1, \ldots, x_n) = \sum_{i=1} \mu_i x_i + \mu_0 \ \in M_1 \Leftrightarrow \mu_i \in M_1^{(1)},\ i = \overline{1,n},\ \mu_0 \in E_2'(\xi). \tag{45}$$

В свою очередь, свойство принадлежности $\mu_i \in M_1^{(1)}$ можно выразить следующим образом: $\mu_i \in M_1^{(1)} \Leftrightarrow \mu_i = a_0 + \xi^2 \mu_i',\ a_0 \in E_2,\ \ \forall\ \ \mu_i' \in E_2'(\xi)$. Другими словами, автомат класса M_1 выглядит так:

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} (a_0^i + \xi^2 \mu_i') x_i + \mu_0 \ \in M_1,\ a_0 \in E_2,\ \ \mu_i',\ \mu_0 \in E_2'(\xi). \tag{46}$$

Докажем, что $K(M) = M_1$. Автоматы f_1, f_2 содержатся в классе M_1, т.к. их коэффициенты при переменных принадлежат классу $M_1^{(1)}$. Автоматы f_3, f_4 — это константы, а классу M_1 принадлежат все константы из $E_2'(\xi)$. Поэтому, в силу K-замкнутости класса M_1, $\ K(M) \subset M_1$.

В $K(M)$ есть нулевой автомат: $Fb_x(f_2(x)) = 0 \in K(M)$.

Проводник также принадлежит K-замыканию множества M:
$f_1(0,0,x) = x \in K(M)$.

Автомат $\xi^3 x$ аналогично выводится из автомата f_1 подстановкой нулевого автомата на его второй и третий входы: $f_1(x,0,0) = \xi^3 x \in K(M)$.

Заметим, что подставив на первый вход автомата f_1 нулевой автомат, мы получим сумматор от двух переменных: $f_1(0, x_2, x_3) = x_2 + x_3 \in K(M)$. То есть достаточно показать, что для любого $\mu \in E_2'(\xi)$ элементы вида $(a_0 + \xi^2 \mu) x$ и μ принадлежат K-замыканию множества M.

Докажем, что для любого многочлена $\tilde{u} \in E_2[\xi]$ в $K(M)$ можно получить автомат вида $\xi^2 x \tilde{u} \in K(M)$, используя математическую индукцию по степени многочлена s. Действительно, для $s = 0$ было показано,что такие автоматы принадлежат K-замыканию множества M:

$$\xi^2 x \cdot 0 = 0 \in K(M); \quad (47)$$

$$\xi^2 x \cdot 1 = \xi^2 x = f_2(x) \in M. \quad (48)$$

Многочлены первой степени:

$$\xi^2 x \cdot \xi = \xi^3 x \in K(M); \quad (49)$$

$$\xi^2 x \cdot (1+\xi) = f_1(x, \xi^2 x, 0) = \xi^3 x + \xi^2 x = \xi^2 x(1+\xi) \in K(M). \quad (50)$$

Пусть для любого многочлена $\tilde{u} = a_0 + a_1\xi + \ldots + a_{s-1}\xi^{s-1}$ степени $s-1$ утверждение верно. Докажем,что соответствующий автомат содержится в $K(M)$ и для любого многочлена степени s. Для этого достаточно показать, что для любого натурального $s \in \mathbb{N}$ автомат $\xi^2 \cdot \xi^s x$ принадлежит K-замыканию множества M (для $s = 1$ доказано выше). Рассмотрим 2 случая:

1) $s = 2 \cdot m,\ m \in \mathbb{N}$. Для этого случая достаточно m раз поставить автомат f_2 в себя:

$$f_2(f_2(\ldots f_2(f_2(x))\ldots) = \xi^2(\xi^2(\ldots\xi^2(\xi^2 x)\ldots) =$$

$$= \xi^2 \cdot \xi^{2\cdot m} x = \xi^2 \cdot \xi^s x \in K(M). \quad (51)$$

2) $s = 2\cdot m + 1,\ \ m \in \mathbb{N}$. Искомый автомат можно получить, подставив в автомат $\xi^3 x$ m раз автомат f_2:

$$\xi^3(f_2(\ldots f_2(f_2(x))\ldots) = \xi^3(\xi^2(\xi^2(\ldots(\xi^2 x)\ldots) =$$

$$= \xi^{2+2(m-1)+3} x = \xi^2 \cdot \xi^s x \in K(M). \quad (52)$$

Очевидно, $2(m-1) + 3 = 2 \cdot m + 1$.

Таким образом, для любого многочлена u степени s (обозначим $u = \tilde{u} + \xi^s$) автомат $\xi^2 x \cdot u$ в $K(M)$ есть:

$$\xi^2 \tilde{u} x + \xi^2 \cdot \xi^s x = \xi^2(\tilde{u} + \xi^s)x = \xi^2 \cdot ux \in K(M). \quad (53)$$

Покажем, что для любого элемента $\mu \in E_2'(\xi)$ автомат $\xi^2 \mu x$ принадлежит K-замыканию множества M. Произвольный элемент из $E_2'(\xi)$ можно представить так:

$$\mu = \frac{u}{1 + \xi \cdot v}, \ \ u, v \in E_2[\xi]. \quad (54)$$

Также рассмотрим 2 случая:

1) $v = 0 + a_1\xi + a_2\xi^2 + \ldots + \xi^s = \xi(a_1 + a_2\xi + \ldots + \xi^{s-1}) = \xi\tilde{v}$. То есть μ имеет следующий вид:

$$\mu = \frac{u}{1 + \xi^2 \cdot \tilde{v}}, \quad u, \tilde{v} \in E_2[\xi]. \tag{55}$$

Тогда сначала подставим в сумматор от двух переменных автоматы $\xi^2 ux$, $\xi^2\tilde{v}x \in K(M)$: $\tilde{f}(x_1, x_2) = \xi^2 ux_1 + \xi^2\tilde{v}x_2 \in K(M)$. После чего применим операцию обратной связи по второй переменной:

$$Fb_{x_2}(\tilde{f}(x_1, x_2)) = \frac{\xi^2 u}{1 + \xi^2\tilde{v}}x_1 = \xi^2\frac{u}{1 + \xi^2\tilde{v}}x_1 = \xi^2\mu x \in K(M). \tag{56}$$

2) $v = 1 + a_1\xi + a_2\xi^2 + \ldots + \xi^s = 1 + \xi\tilde{v}$. Соответствующий элемент $E_2'(\xi)$ выглядит так:

$$\mu = \frac{u}{1 + \xi + \xi^2 \cdot \tilde{v}}, \quad u, \tilde{v} \in E_2[\xi]. \tag{57}$$

Покажем, что вспомогательный автомат $g(x) = \dfrac{1}{1 + \xi^2}x$ содержится в K-замыкании M. Действительно, подставим автомат f_2 на первый вход сумматора от двух переменных и применим по этой переменной операцию обратной связи:

$$g(x) = Fb_{x_1}(\xi^2 x_1 + x_2) = \frac{1}{1 + \xi^2}x_2 \in K(M). \tag{58}$$

Заметим, что для поля E_2 верно $(1+\xi^2) = (1+\xi)^2$. Для рассматриваемого случая сначала подставим на оба входа сумматора от двух переменных автомат $g(x)$:

$$\hat{g}(x_1, x_2) = \frac{1}{1 + \xi^2}x_1 + \frac{1}{1 + \xi^2}x_2 \in K(M). \tag{59}$$

Затем, поскольку для любого многочлена u из кольца $E_2'[\xi]$ доказано, что $\xi^2 ux$ есть в K-замыкании M, то автоматы $\xi^2(1+\xi)\tilde{v}x$ и $\xi^2(1+\xi)ux$ также содержатся в $K(M)$. Подставим их на входы только что полученного автомата $\hat{g}(x_1,\ x_2)$:

$$\tilde{g}(x_1,\ x_2) = \hat{g}(\xi^2(1 + \xi)\tilde{v}x_1,\ \xi^2(1 + \xi)ux_2) = \frac{1}{1 + \xi^2}\Big(\xi^2(1 + \xi)\tilde{v}\Big)x_1 +$$

$$+\frac{1}{1+\xi^2}\left(\xi^2(1+\xi)u\right)x_2 = \frac{\xi^2\tilde{v}}{1+\xi}x_1 + \frac{\xi^2 u}{1+\xi}x_2 \in K(M). \qquad (60)$$

И, наконец, применим операцию обратной связи по первой переменной:

$$Fb_{x_1}(\tilde{g}(x_1,x_2)) = \frac{\xi^2 u}{1+\xi}\cdot\frac{1}{1+\frac{\xi^2\tilde{v}}{1+\xi}}x_2 = \frac{\xi^2 u}{1+\xi}\cdot\frac{1+\xi}{1+\xi+\xi^2\tilde{v}}x_2 =$$

$$= \frac{\xi^2 u}{1+\xi+\xi^2\tilde{v}}x_2 = \xi^2\mu x \in K(M). \qquad (61)$$

Таким образом, для любого $\mu = \xi^2\mu',\ \mu' \in E_2'(\xi)$ доказано, что $\mu\cdot x \in K(M)$. Очевидно, для любого $\mu = 1+\xi^2\mu',\ \ \mu' \in E_2'(\xi)$ соответствующий автомат также есть в $K(M):\ x + \xi^2\mu'\cdot x = (1+\xi^2\mu')x \in K(M)$.

Заметим, что любую константу из $E_2'(\xi)$ можно представить так: $\mu = a_0 + a_1\xi + \xi^2\mu',\ \mu' \in E_2'(\xi),\ a_0, a_1 \in E_2$. Подставив автомат f_3 в автоматы, представленные выше, получим любую константу вида $(a_0 + 0\cdot\xi + \xi^2\mu')$. Если в сумматор от двух переменных подставить на один вход автомат f_4, а на другой вход — константы $(a_0 + 0\cdot\xi + \xi^2\mu')$, то получим в K-замыкании множества M любую константу из $E_2'(\xi)$.

Таким образом, в $K(M)$ есть любой автомат из M_1, т.е. $M_1 \subset K(M)$. И в силу написанного выше получаем, что $K(M) = M_1$.

Покажем, что множество M — это базис класса автоматов M_1. Автомат f_1 является единственным автоматом более, чем от одной переменной, поэтому $K(\{f_2, f_3, f_4\}) \neq M_1$. f_1, f_2, f_4 принадлежат K-замкнутому классу T_0, т.е. $K(\{f_1, f_2, f_4\}) \neq M_1$, а автомат $f_3 \notin T_0$. Автомат с нулевым свободным членом f_2 можно получить только применяя операции композиции к автомату с нулевым свободным членом f_1. Коэффициенты автоматов f_1, f_2 в силу свойств класса M_1 принадлежат $K^{(1)}$-замкнутому классу $M_1^{(1)}$. Несложно показать, что $\xi^2 \notin K^{(1)}(\{1, \xi^3\})$, то получить автомат f_2 в K-замыкании множества $\{f_1, f_3, f_4\}$ нельзя.

Заметим, что, поскольку автоматы f_1, f_2 имеют нулевой свободный член, то и в их K-замыкании можно получить только автомат с нулевым свободным членом. Т.е. используя операции композиции и автоматы из $K(\{f_1, f_2\})$, получить константу можно только, если подставить некоторую константу в автомат из $K(\{f_1, f_2\})$. С другой стороны, так как все коэффициенты при переменных этих автоматов $U(\{f_1, f_2\}) = = \{1, \xi^2, \xi^3\}$ принадлежат $K^{(1)}$-замкнутому классу $M_1^{(1)}$, то и в $K(\{f_1, f_2\})$

автоматы будут иметь коэффициенты при переменных из $M_1^{(1)}$ (в силу замкнутости соответствующих классов). Следовательно, в $K(\{f_1, f_2, f_3\})$ есть только константы из $M_1^{(1)}$. А, т.к. $\xi \notin M_1^{(1)}$, то и константы ξ в K-замыкании множества $\{f_1, f_2, f_3\}$ нет.

Ввиду выше изложенного, приходим к выводу, что множество M является базисом K-замкнутого класса M_1. Лемма полностью доказана.

$\square$

Теорема 1. *Каждый предполный класс линейных автоматов, входящий в А-критериальную систему, является K-конечнопорожденным.*

Доказательство. $\mathcal{J}_A = \{T_0, T_1, V_1, V_2, M_1\}$ — A-критериальная система в L_2. В леммах 1—5 было доказано, что данные классы являются K-конечнопорожденными. Теорема доказана.

$\square$

Следствие 1. *Каждый предполный класс линейных автоматов, входящий в А-критериальную систему, является А-конечнопорожденным.*

Доказательство. Поскольку оператор A-замыкания сильнее оператора K-замыкания, то из K-конечнопорожденности следует A-конечнопорожденность. В теореме 1 было доказано, что каждый класс A-критериальной системы является K-конечнопорожденным и, следовательно, он является A-конечнопорожденным классом автоматов. Следствие доказано.

$\square$

4. Заключение

Таким образом, в настоящей работе был рассмотрен вопрос K- и A- конечнопорожденноти для предполных классов в классе линейных автоматов, функционирующих на полем Галуа, состоящим из двух элементов. Для всех предполных классов, образующих А-критериальную систему было доказано, что они являются К-конечнопорожденными и, следовательно, А-конечнопорожденными. Также для каждого из этих классов был предъявлен базис. В дальнейших публикациях будут представлены результаты решения подобных задач для других предполных классов линейных автоматов.

Автор выражает благодарность своему научному руководителю доценту кафедры МаТИС механико-математического факультета МГУ, д.ф.-м.н. Часовских Анатолию Александровичу за постановку задачи и помощь в исследовании.

Список литературы

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

[2] Клини С. К., "Представление событий в нервных сетях и конечных автоматах", *Автоматы*, 1956, С. 15-67.

[3] Мур Э. Ф., "Умозрительные эксперименты с последовательностными машинами", *Автоматы*, 1956, С. 179-210.

[4] Нейман Дж., "Вероятностная логика и синтез надежных организмов из ненадежных компонент", *Автоматы*, 1956, С. 68-139.

[5] Яблонский С. В., "О построении тупиковых кратных экспериментов для автоматов", *Тр. МИАН СССР*, **133** (1973), С. 263—272.

[6] Лупанов О. Б., "О сравнении двух типов конечных источников", *Проблемы кибернетики*, **9** (1963), С. 321–326.

[7] Кудрявцев В. Б., "Теорема полноты для одного класса автоматов без обратных связей", *Проблемы кибернетики*, **8** (1962), С. 91-115.

[8] Кудрявцев В. Б., "О мощности множеств предполных множеств некоторых функциональных систем, связанных с автоматами", *Проблемы кибернетики*, **13** (1965), С. 45–74.

[9] Часовских А. А., "О полноте в классе линейных автоматов", *Математические вопросы кибернетики*, **3** (1991), С. 140—166.

[10] Часовских А. А., "Проблема А-полноты линейно-автоматных функций над конечным полем", *Интеллектуальные системы. Теория и приложения*, **18**:1 (2014), С. 253—257.

[11] Часовских А. А., "Проблема полноты в классах линейных автоматов", *Интеллектуальные системы. Теория и приложения*, **22**:2 (2018), С. 151-154.

[12] Часовских А. А., "Максимальные подклассы в классах линейных автоматов над конечными полями", *Дискретная математика*, **31**:4 (2019), С. 88-101.

[13] Гилл, А., *Линейные последовательностные машины*, Наука, Москва, 1974, 288 с.

[14] Лидл Р., Нидеррайтер Г., *Конечные поля: в 2 т. Т. 1.*, Мир, Москва, 1988, 430 с.

The problem of K-finite generation for precomplete classes of linear automata constituting an A-criterion system in the space of linear automata.

Biryukova Veronika Andreevna

This article considers the problem of K- and A-finite generation for precomplete classes of linear automata operating over the Galois field consisting of two elements. The set of all studied classes is the A-criterion system in the class of linear automata. A finite basis was presented for each class under consideration.

Keywords: finite automaton, linear automaton, composition operation, feedback operation, completeness, closed class, precomplete class, K-finitely generated class, A-finitely generated class.

References

[1] Kudryavtsev V.B., Alyoshin S.V., Podkolzin A.S., *Introduction to automata theory*, «Science», Moscow, 1985 (In Russian), 320 c.

[2] S.C. Kleene, "Representation of events in nerve nets and finite automata", *Automata Studies*, 1956, 15-67 (In Russian).

[3] E. F. MOORE, "Gedanken-experiments on sequential machines", *Automata Studies*, 1956, 179-210 (In Russian).

[4] J. von Neumann, "Probabilistic logics and the synthesis of reliable organisms from unreliable components", *Automata Studies*, 1956, 68-139 (In Russian).

[5] S. Yablonsky, "On the construction of dead-end multiple experiments for automata", *Proceedings of the Steklov Institute of Mathematics*, **133** (1973), 263—272 (In Russian).

[6] O. Lupanov, "About comparing two types of finite sources", *Problems of cybernetics*, **9** (1963), 321–326 (In Russian).

[7] V. Kudryavtsev, "Completeness theorem for one class of automata without feedback", *Problems of cybernetics*, **8** (1962), 91-115 (In Russian).

[8] V. Kudryavtsev, "The Cardinality of Sets of Precomplete Sets of Some Functional Systems Related to Automata", *Problems of cybernetics*, **13** (1965), 45–74 (In Russian).

[9] Chasovskih A.A, "Completeness in the class of linear automata", *Mathematical problems of cybernetics*, **3** (1991), 140—166 (In Russian).

[10] Chasovskih A.A, “The problem of A-completeness of linear automaton functions over a finite field”, *Intelligent Systems. Theory and Applications*, **18**:1 (2014), 253—257 (In Russian).

[11] Chasovskih A.A, “The problem of completeness in classes of linear automata”, *Intelligent Systems. Theory and Applications*, **22**:2 (2018), 151-154 (In Russian).

[12] Chasovskih A.A., “Maximal subclasses in classes of linear automata over finite fields”, *Discrete Math*, **31**:4 (2019), 88-101 (In Russian).

[13] A. Gill, *Linear Sequential Circuits*, Science, Moscow, 1974 (In Russian), 288 c.

[14] R. Lidl, H. Niederreiter, *Finite Fields, volume 1*, 'World', Moscow, 1988 (In Russian), 430 c.