Проблема полноты линейных дефинитных автоматов

И. В. Молдованов*

В работе исследуется задача полноты в классе линейных дефинитных автоматов над полем из двух элементов относительно операции суперпозиции. Основным результатом является получение критерия полноты для произвольных подмножеств класса линейных дефинитных автоматов, сформулированного в терминах системы замкнутых классов. Полученный критерий обобщает ранее известные результаты, относящиеся к конечнопорожденным подмножествам, содержащим нулевую константу. На его основе доказывается алгоритмическая разрешимость задачи распознавания полноты конечных подмножеств класса линейных дефинитных автоматов.

Ключевые слова: задача полноты, суперпозиция, линейные автоматы, дефинитные автоматы.

1. Введение

Задача исследования полноты естественным образом возникает при изучении функциональных систем. Решение данной проблемы заключается в описании алгоритмических и структурных границ распознаваемости полноты множеств функций для заданной функциональной системы, что позволяет глубже понять свойства рассматриваемых функциональных систем.

С учётом специфики проектирования электронных устройств задача полноты представляет существенный практический интерес применительно к множеству конечных детерминированных автоматов $P_{\text{о.д.}}$, рассматриваемому относительно операций композиции и суперпозиции. Для класса $P_{\text{о.д.}}$ с операциями композиции существуют конечные полные системы. Данный факт позволяет установить критериальность [1] континуальной системы предполных классов, содержащихся в указанном множестве [2]. При этом задача распознавания полноты конечных множеств в этом случае является алгоритмически неразрешимой [3, 4]. В то же время

* *Молдованов Илья Владимирович* — аспирант каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: `jamfr-d@mail.ru`, ORCID: 0009-0004-0595-3350.

Moldovanov Ilia Vladimirovich — graduate student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

класс $P_{\text{о.д.}}$, рассматриваемый относительно операций суперпозиции, не содержит конечных полных систем.

Ввиду структурной сложности множества конечных детерминированных автоматов представляет интерес исследование его подклассов, задаваемых определёнными ограничениями на поведение автоматов. Одним из таких подклассов является класс дефинитных автоматов. Однако задача проверки полноты конечных подмножеств в данном случае также является алгоритмически неразрешимой [5].

В работах [6, 7] были исследованы классы линейных автоматов над конечными полями. Линейные автоматы представляют значительный интерес для вычислительной техники, теории кодирования и в ряде других приложений. Для данных классов были найдены все К-предполные классы [7], а также предложен алгоритм распознавания К-полноты конечных подмножеств [6]. При рассмотрении линейных автоматов относительно операций суперпозиции в [8] было установлено отсутствие конечных полных систем.

Естественным образом возникает класс линейных дефинитных автоматов, который рассматривается в [9]. Данный класс является содержательным подклассом пересечения классов линейных и дефинитных автоматов. Линейным дефинитным автоматом называется автомат, принадлежащий замыканию относительно операций суперпозиции системы, состоящей из задержек с фиксированным начальным состоянием и сумматора. Из представленного определения непосредственно следует, что класс линейных дефинитных автоматов содержит конечные полные системы относительно операций суперпозиции. В работе [10] был получен критерий полноты конечнопорожденных подмножеств данного класса, содержащих нулевую константу, сформулированный в терминах замкнутых классов. Кроме того, в [10] было показано, что на основе указанного критерия может быть построен алгоритм распознавания полноты конечных подмножеств, содержащих нулевую константу. В настоящей работе путём расширения ранее найденной системы замкнутых классов получен критерий полноты произвольных подмножеств класса линейных дефинитных автоматов. Данный критерий может быть использован для построения алгоритма распознавания полноты произвольных конечных подмножеств.

2. Обозначения

Через E_2 обозначим конечное поле из двух элементов $\{0, 1\}$. Через $E_2[\xi]$ обозначим множество многочленов по ξ с коэффициентами из E_2, и $R_2[\xi]$

— множество формальных степенных рядов по ξ:

$$R_2[\xi] = \{\sum_{t=0}^{\infty} a(t)\xi^t \mid a(t) \in E_2\}.$$

В соответствии с [9], отображение $f(x_1, \ldots, x_n) : R_2^n[\xi] \to R_2[\xi]$ будем называть **линейным дефинитным автоматом**, если $\exists\ u_0(\xi), u_1(\xi), \ldots, u_n(\xi) \in E_2[\xi]$ такие, что $\forall \alpha_1, \ldots, \alpha_n \in R_2[\xi]$, имеет место следующее равенство:

$$f(\alpha_1, \ldots, \alpha_n) = \sum_{i=1}^{n} u_i(\xi)\alpha_i + u_0(\xi).$$

Множество всех линейных дефинитных автоматов над E_2 обозначим LD_2. Для некоторого $M \subseteq LD_2$ замыкание данного множества по операциям суперпозиции будем обозначать $S(M)$.

Упорядочим счётное множество всех неприводимых в $E_2[\xi]$ многочленов $p_1, p_2, \ldots$ так, что $p_1 = \xi$. Рассмотрим произвольный неприводимый многочлен p_j степени n_j. Факторкольцо ${}^{E_2[\xi]}\big/_{(p_j)} = P_j$ является полем из 2^{n_j} элементов [11]. Для многочлена $u(\xi) \in E_2[\xi]$ через $\langle u(\xi)\rangle_{(p_j)}$ будем обозначать класс вычетов по модулю p_j, которому он принадлежит.

Для данного поля $P_j = {}^{E_2[\xi]}\big/_{(p_j)}$, $\deg(p_j) = n_j$, рассмотрим все его максимальные подполя. Пусть $n_j = d_1^{k_1} \ldots d_{l_j}^{k_{l_j}}$ — разложение на простые множители. Далее через P_j^s обозначим подполе P_j, содержащее $2^{n_{s,j}}$ элементов, где $n_{j,s} = d_1^{k_1} \ldots d_{s-1}^{k_{s-1}} d_s^{k_s - 1} d_{s+1}^{k_{s+1}} \ldots d_{l_j}^{k_{l_j}}$. Отметим, что множество $\{P_j^s, s \in 1, \ldots, l_j\}$ включает все максимальные собственные подполя и только их [12].

Для пары неприводимых многочленов $p_j, p_{j'}$, $j \neq j'$, $\deg(p_j) = \deg(p_{j'})$, рассмотрим факторкольцо ${}^{E_2[\xi]}\big/_{(p_j p_{j'})}$. Пусть, $\{R_{j,j'}^s\}$ — все подмножества данного кольца, изоморфные P_j и $P_{j'}$. В [10] было показано существование таких множеств.

3. Класс одноместных линейных дефинитных автоматов, сохраняющих ноль

Рассмотрим подмножество LD_2, состоящее из линейных дефинитных автоматов с одним входом, сохраняющих ноль. Обозначим данный класс

$LD_2^{(1)}$. Произвольный автомат, принадлежащий $LD_2^{(1)}$, для некоторого $u(\xi) \in E_2[\xi]$ реализует функцию

$$f(x_1) = u(\xi)x_1, \; u(\xi) \in E_2[\xi].$$

Замыкание некоторого множества $M \subseteq E_2[\xi]$ по операциям сложения и умножения будем обозначать $S^{(1)}(M)$.

Положим $F_+(x_1, x_2) = x_1 + x_2$, автомат, реализующий сумматор. Пусть $\bar{M} \subseteq LD_2^{(1)}$ и $\bar{M}^{(1)} = \{u'(\xi) \mid u'(\xi)x_1 \in \bar{M} \}$. В [6] было показано, что произвольный автомат, содержащийся в замыкании по операциям суперпозиции множества $\bar{M} \cup \{F_+(x_1, x_2)\}$, имеет вид

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} v_i(\xi)x_i, \; v_i(\xi) \in S^{(1)}\left(\bar{M}^{(1)}\right).$$

Поэтому, далее в данном разделе будем рассматривать $E_2[\xi]$ с операциями сложения и умножения.

В работе [6] были получены приведённые ниже результаты.

Определение 1. Определим семейство подмножеств $E_2[\xi]$:

$$RP_j^{(1)} = \{u(\xi) \mid u(\xi) \in E_2[\xi], \; u(\xi) \,\vdots\, p_j(\xi)\}, \; j \in \mathbb{N},$$
$$MP_j^{(1)} = \{u(\xi) \mid u(\xi) \in E_2[\xi], \; (u(\xi) + u(0)) \,\vdots\, \xi p_j\}, \; j \in \mathbb{N}.$$

Обозначим $JP^{(1)} = \{RP_j^{(1)} \mid j \in \mathbb{N}\} \cup \{MP_j^{(1)} \mid j \in \mathbb{N}\}$.

Лемма 1. *Пусть $M \subseteq E_2[\xi]$. Если $M \not\subseteq \Theta, \; \forall \Theta \in JP^{(1)}$, то существует $V(\xi) \in E_2[\xi], \; V(\xi) \neq 0$, такой, что $\forall v(\xi) \in E_2[\xi]$ многочлен $V(\xi) \cdot v(\xi) \in S^{(1)}(M)$.*

На основании леммы 1 в [10] было сформулировано следующее утверждение, которое согласуется с известными результатами [13], [14], [15].

Определение 2. Определим семейство подмножеств $E_2[\xi]$:

$$L_{j,s}^{(1)} = \{u(\xi) \mid u(\xi) \in E_2[\xi], \langle u(\xi)\rangle_{(p_j)} \in P_j^s\}, \; j \in \mathbb{N},$$
$$N_j^{(1)} = \{v^2(\xi) + p_j^2 u(\xi) \mid v(\xi), u(\xi) \in E_2[\xi], \; \deg(v(\xi)) < \deg(p_j)\}, \; j \in \mathbb{N},$$
$$I_{j,j',s}^{(1)} = \{u(\xi) \mid u(\xi) \in E_2[\xi], \; \langle u(\xi)\rangle_{(p_j p_{j'})} \in R_{j,j'}^s\}, \; j \in \mathbb{N}, \; j' \in \mathbb{N}, \; j > j',$$
$$\deg(p_j) = \deg(p_{j'}).$$

Обозначим $H^{(1)} = \{L_{j,s}^{(1)}\} \cup \{N_j^{(1)}\} \cup \{I_{j,j',s}^{(1)} \}$.

Теорема 1. *Пусть $M \subseteq E_2[\xi]$. $S^{(1)}(M) = E_2[\xi] \iff M \not\subseteq \Theta, \; \forall \Theta \in JP^{(1)} \cup H^{(1)}$.*

4. Выразимость сумматора и задержки с добавками

Рассмотрим два автомата

$$\tilde{F}_{+}(x_1, x_2, z) = x_1 + x_2 + \tilde{F}'_{+}(z),\ \tilde{F}_{\xi}(x_1, z) = \xi x_1 + \tilde{F}'_{\xi}(z),$$

где $\tilde{F}'_{+}(z),\ \tilde{F}'_{\xi}(z)$ принадлежат LD_2. Данные автоматы, с точностью до некоторой добавки, реализуют сумматор от двух переменных и задержку с нулевым начальным состоянием, соответственно. Обозначим через $\tilde{A}$ множество пар $\{\{x_1 + x_2 + \tilde{F}'_{+}(z),\ \xi x_1 + \tilde{F}'_{\xi}(z)\} \mid \tilde{F}'_{+}(z),\ \tilde{F}'_{\xi}(z) \in LD_2\}$, а через $\tilde{S}(M)$ — множество $\{\{f_1,\ f_2\} \mid f_1,\ f_2 \in S(M)\}$. Если для $M \subseteq LD_2$ имеем $\tilde{S}(M) \cap \tilde{A} \neq \varnothing$, то будем говорить, что $\tilde{F}_{+}(x_1, x_2, z),\ \tilde{F}_{\xi}(x_1, z) \in S(M)$ для некоторых добавок $\tilde{F}'_{+}(z),\ \tilde{F}'_{\xi}(z) \in LD_2$.
Обозначим $U(f)$ — множество коэффициентов при переменных автомата $f \in LD_2$.

Определение 3. Определим семейство подмножеств LD_2:

$$\begin{aligned}
L_{j,s} &= \{\ f \mid f \in LD_2,\ U(f) \subset L^{(1)}_{j,s}\},\ j \in \mathbb{N},\\
N_j &= \{\ f \mid f \in LD_2,\ U(f) \subset N^{(1)}_{j}\},\ j \in \mathbb{N},\\
I_{j,j',s} &= \{\ f \mid f \in LD_2,\ U(f) \subset I^{(1)}_{j,j',s}\},\ j \in \mathbb{N},\ j' \in \mathbb{N},\\
&\qquad j > j',\ \deg(p_j) = \deg(p_{j'}),\\
V_j &= \{\ f \mid f \in LD_2,\ f = \sum_{i=1}^{n} u_i(\xi) x_i + u_0(\xi) \text{ и среди}\\
&\qquad \text{многочленов } u_i(\xi) \text{ существует не более одного такого, что}\\
&\qquad p_j \nmid u_i(\xi)\}, \qquad j \in \mathbb{N},\\
P_J &= \{\ f \mid f \in LD_2,\ f = \sum_{i=1}^{n} u_i(\xi) x_i + u_0(\xi) \text{ и } \forall\ \{j, j'\} \subset J,\\
&\qquad j \neq j',\ \nexists\ u_i(\xi), u_{i'}(\xi) \in U(f),\ i \neq i',\ \text{таких, что}\\
&\qquad p_j \nmid u_i(\xi),\ p_{j'} \nmid u_{i'}(\xi)\}, \qquad J \subset \mathbb{N},\ 2 \leqslant |J| < \infty,\\
\bar{P} &= \{\ f \mid f \in LD_2,\ f = \sum_{i=1}^{n} u_i(\xi) x_i + u_0(\xi) \text{ и } n = 1\\
&\qquad \text{или } \exists\ p_j \text{ такой, что } U(f) \subset \langle 0 \rangle_{(p_j)}\}.
\end{aligned}$$

Обозначим $\bar{H} = \{L_{j,s}\} \cup \{N_j\} \cup \{I_{j,j',s}\ \} \cup \{V_j\} \cup \{P_J\} \cup \{\bar{P}\}$.
Σ-замкнутость в LD_2 всех классов кроме $\bar{P}$ показана в [10].

Лемма 2. *Множество $\bar{P}$ замкнуто в LD_2 относительно операций суперпозиции.*

Доказательство. Переименование переменных и подстановка, очевидно, не выводят за пределы данного класса. Отождествление переменных применимо только в случае $n > 1$, то есть существует неприводимый многочлен p_j, который делит коэффициент при любой переменной автомата, следовательно, p_j также делит сумму произвольных коэффициентов. $\square$

Положим $H = \bar{H} \setminus \{\bar{P}\}$. Пусть $M \subset LD_2$ — конечно порождённое. В работе [10] было показано, что если $M \nsubseteq \Theta$, $\forall \Theta \in H$, то $\tilde{S}(M) \cap \tilde{A} \neq \varnothing$. Также в [10] были доказаны следующие утверждения, представленные ниже в качестве лемм.

Лемма 3. *Пусть $M \subseteq LD_2$. Если $M \nsubseteq \Theta$, $\forall \Theta \in \{L_{1,0}, L_{1,1}\} \cup \{N_1\} \cup \{V_1\}$, то $\exists u_1(\xi) \in E_2[\xi]$, $Q_1'(z) \in LD_2$, что автомат*

$$Q_1(x_1, z) = (\xi + \xi^2 u_1(\xi))x_1 + Q_1'(z),$$

содержится в $S(M)$.

Лемма 4. *Пусть $M \subseteq LD_2$, $D = \{p_{j_1}, \ldots, p_{j_K}\}$, $K > 1$, — конечное множество неприводимых многочленов и $\xi \in D$. Если $M \nsubseteq \Theta$, $\forall \Theta \in \{L_{j,s} \mid p_j \in D\} \cup \{N_j \mid p_j \in D\} \cup \{V_j \mid p_j \in D\} \cup \{I_{j,j',s} \mid \deg(p_j) = \deg(p_{j'}),\ p_j, p_{j'} \in D\} \cup \{P_{\{j,j'\}},\ p_j, p_{j'} \in D\}$, то $\forall p_j \in D$, $\exists u_j(\xi) \in E_2[\xi]$, $Q_j'(z) \in LD_2$, что автомат*

$$Q_j(x_1, z) = (\xi + \xi p_j u_j(\xi))x_1 + Q_j'(z),$$

содержится в $S(M)$.

Лемма 5. *Пусть $M \subseteq LD_2$ и $D = \{p_{j_1}, \ldots, p_{j_K}\}$, $K \geqslant 1$ — конечное множество неприводимых многочленов. Если $M \nsubseteq \Theta$, $\forall \Theta \in \{V_j \mid p_j \in D\} \cup \{P_J \mid J \subset \mathbb{N},\ |J| > 1,\ \ p_j \in D \iff j \in J\}$, то найдутся $u_i(\xi) \in E_2[\xi]$, $p_{j_i} \nmid u_i(\xi)$, $i = 1, \ldots, K$, такие что $\forall s \in \mathbb{N}$, $\exists H_{D,s}'(z) \in LD_2$, для которого*

$$H_{D,s}(x_{1,1}, \ldots, x_{2^s,1}, \ldots, x_{1,K}, \ldots, x_{2^s,K}, z) = \sum_{i=1}^{K} \sum_{l=1}^{2^s} u_i^{2^{s-1}}(\xi) x_{i,l} + H_{D,s}'(z)$$

принадлежит $S(M)$.

Покажем, что система $\bar{H}$, получающаяся из H добавлением класса $\bar{P}$, является критериальной относительно проверки соотношения $\tilde{S}(M) \cap \tilde{A} \neq \varnothing$ для подмножеств $M \subseteq LD_2$.

Пусть $u(\xi) \in E_2[\xi]$, $u(\xi) \neq 0$, тогда обозначим $D(u(\xi)) = \{p_j \mid u(\xi) \vdots p_j\}$.

Лемма 6. *Пусть $M \subseteq LD_2$. Если $M \nsubseteq \bar{P}$, то найдутся $m(\xi) \in E_2[\xi]$ и $n \in \mathbb{N}, \{v_i(\xi) \mid i = 1, \ldots, n\} \subset E_2[\xi]$, что для произвольного $T = 2^t,\ t \in \mathbb{N}$ автомат*

$$B_T(x_1, \ldots, x_n, y_1, \ldots, y_T, z) = \sum_{i=1}^{n} v_i(\xi)x_i + \sum_{l=1}^{T} m^T(\xi)y_l + B'_T(z),$$

$$\textit{НОД}(v_i(\xi),\ i = 1, \ldots, n)) = 1,\ D(m(\xi)) \subseteq \bigcup_{i=1}^{n} D(v_i(\xi)),\ n \geqslant 2,$$

принадлежит $S(M)$.

Доказательство. По условию в множестве $M \setminus \bar{P}$ содержится автомат

$$B(x_1, \ldots, x_n) = \sum_{i=1}^{n} u_i(\xi)x_i + u_0(\xi),\ \text{НОД}\,(u_i(\xi),\ i = 1, \ldots, n)) = 1,\ n \geqslant 2.$$

Обозначим $Z^k,\ k \in \mathbb{Z}_+$ — набор, состоящий из k идущих подряд переменных z, и рассмотрим подстановку

$$\bar{B}(x_1, \ldots, x_n, y_1, y_2, z) = B(B(x_1, y_1, Z^{n-2}), B(y_2, x_2, Z^{n-2}), x_3, \ldots, x_n) =$$
$$u_1^2(\xi)x_1 + u_2^2(\xi)x_2 + \sum_{i=3}^{n} u_i(\xi)x_i + u_1(\xi)u_2(\xi)y_1 + u_1(\xi)u_2(\xi)y_2 + \bar{B}'(z) =$$
$$\sum_{i=1}^{n} u'_i(\xi)x_i + m(\xi)y_1 + m(\xi)y_2 + \bar{B}'(z).$$

По построению автомата $\bar{B}$, имеем

$$\text{НОД}\left(\{u'_i(\xi),\ i = 1, \ldots, n)\}\right) = 1,\ D(m(\xi)) \subseteq \bigcup_{i=1}^{n} D(u'_i(\xi)),\ n \geqslant 2.$$

Индукцией по $t \in \mathbb{N}$ докажем утверждение леммы. База индукции реализуется

$$B_2 = \bar{B}(x_1, \ldots, x_n, \bar{B}(Z^n, y_1, y_2, z), z, z) \in S(M).$$

В качестве шага индукции рассмотрим подстановку

$$B_{2T}(x_1, \ldots, x_n, y_1, \ldots, y_{2T}, z) =$$
$$B_T(x_1, \ldots, x_n, B_T(Z^n, y_1, \ldots, y_T, z), B_T(Z^n, y_{T+1}, \ldots, y_{2T}, z), Z^{T-2}, z)$$
$$\in S(M).$$

□

Лемма 7. *Пусть* $M \subseteq LD_2$. *Если* $\forall \Theta,\ \Theta \in \bar{H}$ *имеем* $M \not\subseteq \Theta$, *то для некоторого* $V(\xi) \in E_2[\xi],\ V(\xi) \neq 0$ *и произвольного* $v(\xi) \in E_2[\xi]$, *найдётся автомат* $U_{v(\xi)}(x_1, z) \in S(M)$, *что для некоторого* $U'_{v(\xi)}(z) \in LD_2$ *выполнено*

$$U_{v(\xi)}(x_1, z) = v(\xi)V(\xi)x_1 + U'_{v(\xi)}(z) \in S(M).$$

Доказательство. По условию $M \not\subseteq \bar{P}$, следовательно по лемме 6 существуют $m(\xi) \in E_2[\xi]$ и $n \in \mathbb{N}, \{u_i(\xi) \mid i = 1, \ldots, n\} \subset E_2[\xi]$, что автомат

$$\begin{gathered} B_T(x_1, \ldots, x_n, y_1, \ldots, y_T, z) = \sum_{i=1}^{n} u_i(\xi)x_i + \sum_{l=1}^{T} m^T(\xi)y_l + B'_T(z), \\ \text{НОД}\,(u_i(\xi),\ i = 1, \ldots, n)) = 1,\ D(m(\xi)) \subseteq \bigcup_{i=1}^{n} D(u_i(\xi)),\ n \geqslant 2, \end{gathered} \tag{1}$$

принадлежит $S(M)$ для произвольного $T = 2^t,\ t \in \mathbb{N}$.
Многочлен $m(\xi)$, участвующий в выражении (1), имеет вид $m(0) + \xi m'(\xi)$. Если $m(0) = 0$, то положим $D_1 = \varnothing,\ S_1 = 0$, иначе $D_1 = D(m'(\xi)) \cup \{\xi\},\ S_1 = |D_1|$. Для некоторого $T_1 \geqslant 2(S_1 + 1),\ T_1 = 2^t,\ t \in \mathbb{N}$ рассмотрим автомат B_{T_1}. Обозначим $\bar{X}^{k_1}, \bar{Y}_1^{k_2}, \bar{Y}_2^{k_3},\ k_1, k_2, k_3 \in \mathbb{N}$ — наборы идущих подряд и последовательно-пронумерованных переменных x_* и $y_{*,1},\ y_{*,2}$, соответственно:

$$B_{T_1}(\bar{X}^n, \bar{Y}_1^{T_1/2}, \bar{Y_2}^{T_1/2}, z) = \sum_{i=1}^{n} u'_i(\xi)x_i + \sum_{l=1}^{T_1/2} m^{T_1}(\xi)y_{l,1} + \sum_{l=1}^{T_1/2} m^{T_1}(\xi)y_{l,2} + B'_{T_1}(z).$$

Имеем $D_1 = \{p_{j_1}, \ldots, p_{j_{S_1}}\}$. По леммам 3 и 4 для любого $p_j \in D_1$, $\exists q_j(\xi) \in E_2[\xi],\ Q'_j(z) \in LD_2$, что автомат

$$Q_j(x_1, z) = (\xi + \xi p_j q_j(\xi))x_1 + Q'_j(z),$$

содержится в $S(M)$.
Рассмотрим подстановку

$$\begin{gathered} \tilde{B}(\bar{X}^n, \bar{Y}_1^{S_1+1}, \bar{Y_2}^{S_1+1}, z) = B_{T_1}(\bar{X}^n, Q_{j_1}(y_{1,1}, z), \ldots, Q_{j_{S_1}}(y_{S_1,1}, z), y_{S_1+1,1}, \\ Q_{j_1}(y_{1,2}, z), \ldots, Q_{j_{S_1}}(y_{S_1,2}, z), y_{S_1+1,2}, z) = \sum_{i=1}^{n} u'_i(\xi)x_i + \sum_{l=1}^{S_1} w_l(\xi)y_{l,1} + \\ + \sum_{l=1}^{S_1} w_l(\xi)y_{l,2} + m^{T_1}(\xi)y_{S_1+1,1} + m^{T_1}(\xi)y_{S_1+1,2} + \tilde{B}'(z) \in S(M). \end{gathered}$$

В случае если $m(0)=1$, то $m^{2^s}(\xi)=m(0)^{2^s}+(\xi m'(\xi))^{2^s}$ в поле характеристики 2, следовательно, для произвольного p_{j_l}, $p_{j_l}\in D_1$ имеем

$$w_l(\xi)=\big(1+\xi p_{j_l}m''(\xi)\big)\cdot(\xi+\xi p_{j_l}q_{j_l}(\xi))=\xi(p_{j_l}w_l''(\xi)+1)\notin MP^{(1)}_{j_l}. \quad (2)$$

Из выражений (1) и (2) следует

$$U(\tilde{B}(\bar{X}^n,\bar{Y}_1^{S_1+1},\bar{Y}_2^{S_1+1},z))\nsubseteq\Theta,\ \forall\Theta\in JP^{(1)},$$

и все коэффициенты при переменных набора $\bar{Y}_1$ продублированы коэффициентами при переменных набора $\bar{Y}_2$.

Положим $D_2=\bigcup\limits_{i=1}^{n}D(u_i(\xi))$, $S_2=|D_2|$, тогда лемме 5 $S(M)$ принадлежит автомат

$$H_1(\bar{X_1}^{S_2},\bar{X_2}^{S_2},z)=\sum_{i=1}^{S_2}(\tilde{u}_i(\xi)x_{i,1}+\tilde{u}_i(\xi)x_{i,2})+H_1'(z),\ p_{j_i}\nmid\tilde{u}_i(\xi),\ p_{j_i}\in D_2. \quad (3)$$

Рассмотрим подстановку

$$\tilde{B}(\underbrace{H_1(\bar{X_1}^{S_2},\bar{X_2}^{S_2},z),\ldots,H_1(\bar{X_1}^{S_2},\bar{X_2}^{S_2},z)}_{n\text{ раз}},\bar{Y}_1^{S_1+1},\bar{Y_2}^{S_1+1},z).$$

Из выражений (1) и (3) следует, что отождествлением части переменных наборов $\bar{X}_1$ и $\bar{X}_2$ в переменную z, полученный автомат можно привести к виду

$$\hat{B}(\bar{X_1}^{S_2},\bar{X_2}^{S_2},\bar{Y}_1^{S_1+1},\bar{Y_2}^{S_1+1},z)=\sum_{i=1}^{S_2}\hat{u}_i(\xi)x_{i,1}+\sum_{i=1}^{S_2}\hat{u}_i(\xi)x_{i,2}+$$
$$+m^{\bar{S}_1}(\xi)y_{S_1+1,1}+m^{\bar{S}_1}(\xi)y_{S_1+1,2}+\sum_{l=1}^{S_1}w_l(\xi)y_{l,1}+\sum_{l=1}^{S_1}w_l(\xi)y_{l,2}+\hat{B}'(z),$$
$$p_{j_i}\nmid\hat{u}_i(\xi),\ p_{j_i}\in D_2,\ D(m(\xi))\subseteq D_2.$$

Имеем

$$\hat{B}(\bar{X_1}^{S_2},\bar{X_2}^{S_2},\bar{Y}_1^{S_1+1},\bar{Y_2}^{S_1+1},z)\in S(M),$$
$$U(\hat{B}(\bar{X_1}^{S_2},\bar{X_2}^{S_2},\bar{Y}_1^{S_1+1},\bar{Y_2}^{S_1+1},z))\nsubseteq\Theta,\ \forall\Theta\in JP^{(1)}$$

и все коэффициенты при переменных наборов $\bar{X}_1$ и $\bar{Y}_1$ продублированы коэффициентами при соответствующих переменных наборов $\bar{X}_2$ и $\bar{Y}_2$. В [10] было показано, что из описанных выше условий и леммы 1 следует утверждение данной леммы. □

Докажем основное утверждение раздела — критерий принадлежности сумматора и задержки, с точностью до некоторых добавок, Σ-замыканию произвольного подмножества LD_2.

Теорема 2. *Пусть $M \subseteq LD_2$. Если $M \nsubseteq \Theta,\ \forall \Theta \in \bar{H}$, то $\tilde{S}(M) \cap \tilde{A} \neq \varnothing$.*

Доказательство. По лемме 6 автомат

$$\begin{gathered} P(\bar{X}^n, y_1, y_2, z) = \sum_{i=1}^{n} u_i(\xi)x_i + m(\xi)y_1 + m(\xi)y_2 + P'(z), \\ \text{НОД}\,(\{u_i(\xi),\ i = 1, \ldots, n)\}) = 1,\ D(m(\xi)) \subseteq \bigcup_{i=1}^{n} D(u_i(\xi)),\ n \geqslant 2. \end{gathered} \tag{4}$$

принадлежит $S(M)$.
По лемме 7 $\exists\ V(\xi) \in E_2[\xi]$, такой, что $\forall\ v(\xi) \in E_2[\xi]$ автомат

$$U_{v(\xi)}(x_1, z) = v(\xi)V(\xi)x_1 + U'_{v(\xi)}(z) \in S(M). \tag{5}$$

Положим $D = \bigcup\limits_{i=1}^{n} D(u_i(\xi)) \cup D(V(\xi)) = \{p_{j_1}, \ldots, p_{j_T}\},\ T = |D|$. Для фиксированного $i,\ p_{j_i} \in D$ обозначим

$$Cl_i = \{L_{j_i,k}\} \cup \{N_{j_i}\} \cup \{V_{j_i}\} \cup \{I_{j_i,j_{i'},k} \mid \deg(p_{j_i}) = \deg(p_{j_{i'}}),\ p_{j_{i'}} \in D\}.$$

Пусть $T' = \max\limits_{i=1}^{T} |Cl_i|$, тогда по лемме 5 для некоторого $\bar{T} \geqslant 4(T'+1),\ \bar{T} = 2^t,\ t \in \mathbb{N}$ автомат

$$H_{D,t}(\bar{X}^{T\cdot\bar{T}}, z) = \sum_{i=1}^{T}\sum_{k=1}^{\bar{T}} \bar{u}_i^{\bar{T}/2}(\xi)x_{(i-1)\bar{T}+k} + H'_{D,t}(z),\ p_{j_i} \nmid \bar{u}_i(\xi),\ p_{j_i} \in D$$

принадлежит $S(M)$. Положим $\hat{T} = \bar{T}/4$ и переименуем переменные данного автомата следующим образом

$$\begin{gathered} H(\bar{X}_1^{T\hat{T}}, \bar{X}_2^{T\hat{T}}, \bar{X}_3^{T\hat{T}}, \bar{X}_4^{T\hat{T}}, z) = \sum_{i=1}^{T}\sum_{k=1}^{\hat{T}} \bar{u}_i^{\bar{T}/2}(\xi)x_{(i-1)\hat{T}+k,1} + \\ + \sum_{i=1}^{T}\sum_{k=1}^{\hat{T}} \bar{u}_i^{\bar{T}/2}(\xi)x_{(i-1)\hat{T}+k,2} + \sum_{i=1}^{T}\sum_{k=1}^{\hat{T}} \bar{u}_i^{\bar{T}/2}(\xi)x_{(i-1)\hat{T}+k,3} + \\ \sum_{i=1}^{T}\sum_{k=1}^{\hat{T}} \bar{u}_i^{\bar{T}/2}(\xi)x_{(i-1)\hat{T}+k,4} + H'(z),\ p_{j_i} \nmid \bar{u}_i(\xi),\ p_{j_i} \in D. \end{gathered} \tag{6}$$

Рассмотрим подстановку

$$P(H(\bar{X}_1^{T\hat{T}}, \bar{X}_2^{T\hat{T}}, \bar{X}_3^{T\hat{T}}, \bar{X}_4^{T\hat{T}}, z), \ldots, H(\bar{X}_1^{T\hat{T}}, \bar{X}_2^{T\hat{T}}, \bar{X}_3^{T\hat{T}}, \bar{X}_4^{T\hat{T}}, z), y_1, y_2, z).$$

Из выражений (4) и (6) следует, что, используя операцию отождествления переменных, из данного автомата можно получить автомат:

$$\begin{gathered}\tilde{P}(\bar{X}_1^{T\hat{T}}, \bar{X}_2^{T\hat{T}}, \bar{X}_3^{T\hat{T}}, \bar{X}_4^{T\hat{T}}, y_1, y_2, z) = \sum_{i=1}^{T}\sum_{k=1}^{\hat{T}} \tilde{u}_i^{\bar{T}/2}(\xi) x_{(i-1)\hat{T}+k,1} + \\ \sum_{i=1}^{T}\sum_{k=1}^{\hat{T}} \tilde{u}_i^{\bar{T}/2}(\xi) x_{(i-1)\hat{T}+k,2} + \sum_{i=1}^{T}\sum_{k=1}^{\hat{T}} \tilde{u}_i^{\bar{T}/2}(\xi) x_{(i-1)\hat{T}+k,3} + \\ \sum_{i=1}^{T}\sum_{k=1}^{\hat{T}} \tilde{u}_i^{\bar{T}/2}(\xi) x_{(i-1)\hat{T}+k,4} + m(\xi)y_1 + m(\xi)y_2 + \tilde{P}'(z), \\ p_{j_i} \nmid \tilde{u}_i(\xi),\ p_{j_i} \in D,\ D(m(\xi)) \cup D(V(\xi)) \subseteq D.\end{gathered} \tag{7}$$

Рассмотрим $Cl_i = \{\Theta_{1,i}^{(1)}, \ldots, \Theta_{L_i,i}^{(1)}\},\ L_i \leqslant \hat{T},\ i = 1, \ldots, T$. По условию теоремы и по определению классов, принадлежащих сериям $L_{j,s}, N_j, I_{j,j',s}$, для любой пары $(k,i),\ i = 1, \ldots, T,\ k = 1, \ldots, L_i$ и некоторого $q_{k,i}(\xi) \in E_2[\xi],\ q_{k,i}(\xi) \notin \Theta_{k,i}^{(1)}$ автомат

$$Q_{k,i}(x_1, z) = q_{k,i}(\xi)x_1 + Q'_{k,i}(z),$$

принадлежит $S(M)$. Рассмотрим симметричную относительно наборов переменных $\bar{X}_1^{T\hat{T}}, \bar{X}_2^{T\hat{T}}, \bar{X}_3^{T\hat{T}}$ и $\bar{X}_4^{T\hat{T}}$ подстановку. Опишем только преобразования переменных, входящих в $\bar{X}_1^{T\hat{T}}$. Данный набор разобьём на подгруппы $\bar{X}_{1,1}^{\hat{T}}, \ldots, \bar{X}_{T,1}^{\hat{T}}$, имеем

$$\begin{gathered}\hat{P}(\bar{X}_{1,1}^{L_1}, \ldots, \bar{X}_{T,1}^{L_T}, \ldots, y_1, y_2, z) = \\ \tilde{P}(\sigma_{1,1,1}, \ldots, \sigma_{\hat{T},1,1}, \ldots, \sigma_{1,T,1}, \ldots, \sigma_{\hat{T},T,1}, \ldots, y_1, y_2, z).\end{gathered}$$

Внутри подгруппы с номером $i,\ 1 \leqslant i \leqslant T$ определим подстановку по следующему правилу:

$$\sigma_{k,i,1} = \begin{cases} Q_{k,i}(x_{k,i,1}, z), & 1 \leqslant k \leqslant L_i \\ x_{k,i,1}, & k = L_i + 1 \\ z, & L_i + 1 < k \leqslant \hat{T} \end{cases}.$$

Таким образом, учитывая соотношение $\hat{T} \geqslant L_i + 1,\ i = 1, \ldots, T$, каждая подгруппа заканчивается набором из $\hat{T} - L_i - 1$ переменных z. Имеем

$$\begin{aligned}
&\hat{P}(\bar{X}_{1,1}^{L_1+1}, \ldots, \bar{X}_{T,1}^{L_T+1}, \ldots, y_1, y_2, z) = \\
&= \tilde{P}(Q_{1,1}(x_{1,1,1}, z), \ldots, Q_{L_1,1}(x_{L_1,1,1}, z), x_{L_1+1,1,1}, Z^{\hat{T}-L_1-1}, \ldots, \\
&\quad Q_{1,T}(x_{1,T,1}, z), \ldots, Q_{L_T,T}(x_{L_T,T,1}, z), x_{L_T+1,T,1}, Z^{\hat{T}-L_T-1}, \ldots, y_1, y_2, z) = \\
&= \sum_{i=1}^{T}\left(\sum_{k=1}^{L_i} w_{k,i}(\xi)x_{k,i,1} + x_{k,L_i+1,1}\right) + \sum_{i=1}^{T}\left(\sum_{k=1}^{L_i} w_{k,i}(\xi)x_{k,i,2} + x_{k,L_i+1,2}\right) + \\
&+ \sum_{i=1}^{T}\left(\sum_{k=1}^{L_i} w_{k,i}(\xi)x_{k,i,3} + x_{k,L_i+1,3}\right) + \sum_{i=1}^{T}\left(\sum_{k=1}^{L_i} w_{k,i}(\xi)x_{k,i,4} + x_{k,L_i+1,4}\right) + \\
&+ m(\xi)y_1 + m(\xi)y_2 + \hat{P}'(z), \qquad w_{k,i}(\xi) \notin \Theta_{k,i}^{(1)},\ D(m(\xi)) \cup D(V(\xi)) \subseteq D.
\end{aligned}$$

Для обозначенного автомата выполнено

$$\begin{aligned}
U(\hat{P}(...)) \nsubseteq \Theta, \quad &\forall \Theta \in \{L_{j,s} \mid p_j \in D\} \cup \{N_j \mid p_j \in D\} \cup \\
&\cup \{V_j \mid p_j \in D\} \cup \{I_{j,j',s} \mid \deg(p_j) = \deg(p_{j'}),\ p_j, p_{j'} \in D\}.
\end{aligned} \tag{8}$$

В работе [10] было показано, что из выражения (8) следует, что для любых $\{n_1, \ldots, n_T \mid n_i \in \mathbb{N}\},\ r(\xi) \in E_2[\xi],\ \deg(r(\xi)) < \sum_{i=1}^{T} n_i \deg(p_{j_i}),\ p_{j_i} \in D$ и некоторых $w_{r(\xi)}(\xi) \in E_2[\xi],\ B'_{r(\xi)}(z) \in LD_2$ автомат

$$\begin{aligned}
B_{r(\xi)}(x_1, x_2, y_1, y_2, z) = &\left(r(\xi) + w_{r(\xi)}(\xi)\prod_{i=1}^{T} p_{j_i}^{n_i}\right)x_1 + \\
&+ \left(r(\xi) + w_{r(\xi)}(\xi)\prod_{i=1}^{T} p_{j_i}^{n_i}\right)x_2 + m(\xi)y_1 + m(\xi)y_2 + B'_{r(\xi)}(z) \in S(M).
\end{aligned}$$

Так как $D(m(\xi)) \cup D(V(\xi)) \subseteq D$ из выражения (7), то подстановкой автоматов вида (5) вместо переменных y_1 и y_2, можно показать, что автоматы

$$\begin{aligned}
\tilde{F}_+(x_1, x_2, y_1, y_2, z) &= \left(1 + w_{1(\xi)}(\xi)\prod_{i=1}^{T} p_{j_i}^{n_i}\right)x_1 + \left(1 + w_{1(\xi)}(\xi)\prod_{i=1}^{T} p_{j_i}^{n_i}\right)x_2 \\
&\quad + w_{1(\xi)}(\xi)\prod_{i=1}^{T} p_{j_i}^{n_i} y_1 + w_{1(\xi)}(\xi)\prod_{i=1}^{T} p_{j_i}^{n_i} y_2 + \tilde{F}'_+(z), \\
\tilde{F}_\xi(x_1, y_1, z) &= \left(\xi + w_\xi(\xi)\prod_{i=1}^{T} p_{j_i}^{n_i}\right)x_1 + w_\xi(\xi)\prod_{i=1}^{T} p_{j_i}^{n_i} y_1 + \tilde{F}'_\xi(z),
\end{aligned}$$

принадлежат $S(M)$. Отождествление соответствующих пар переменных x_1, y_1 и x_2, y_2, завершает доказательство теоремы. $\square$

5. Выразимость константы 0

Пронумеруем элементы поля P_j, $\deg(p_j) = n_j$ в двоичном порядке по коэффициентам их представителей в полиномиальном базисе $(1, \xi, \ldots, \xi^{n_j-1})$. Для

$$s = \sum_{k=0}^{n_j-1} a_k 2^k,\ a_k \in \{0,1\},$$

положим

$$\langle r_s(\xi)\rangle_{(p_j)} = \langle \sum_{k=0}^{n_j-1} a_k \xi^k \rangle_{(p_j)}.$$

Определение 4. Определим семейство подмножеств LD_2:

$$\begin{aligned} S_{j,s} = \{\ f \mid f \in LD_2,\ f = \sum_{i=1}^{n} u_i(\xi)x_i + u_0(\xi) \text{ и} \\ \forall v_1, \ldots, v_n \in \langle r_s(\xi)\rangle_{(p_j)} \text{ имеем} \\ \left(\sum_{i=1}^{n} u_i(\xi)v_i(\xi) + u_0(\xi)\right) \in \langle r_s(\xi)\rangle_{(p_j)}\}, j \in \mathbb{N},\ s = 1, \ldots, 2^{\deg(p_j)}, \end{aligned}$$

$$U_j = \{\ f \mid f \in LD_2,\ f = \sum_{i=1}^{n} u_i(\xi)x_i + u_0(\xi) \text{ и } \left(\sum_{i=1}^{n} u_i(\xi)\right) \in \langle 1\rangle_{(p_j)}\},$$
$$j \in \mathbb{N}.$$

Обозначим $H_0 = \{S_{j,s} \mid j \in \mathbb{N}, s = 1, \ldots, 2^{\deg(p_j)}\} \cup \{U_j \mid j \in \mathbb{N}\}$.

Лемма 8. *Для любого $\Theta \in H_0$ множество Θ замкнуто в LD_2 относительно операций суперпозиции.*

Доказательство. Зафиксируем $j \in \mathbb{N}$ и рассмотрим классы $S_{j,s}$ и U_j. Операция переименования переменных не выводит за пределы обозначенных классов, так как не изменяет коэффициенты при переменных автомата.
Рассмотрим операцию отождествления. Отображение $E_2[\xi] \to E_2[\xi] \big/ (p_j)$,

которое ставит в соответствие многочлену его остаток по модулю неприводимого многочлена p_j, является гомоморфизмом, следовательно, сложение коэффициентов при переменных не выводит за пределы класса Θ, $\forall \Theta \in H_0$.

Рассмотрим операцию подстановки. Пусть, без ограничения общности, автомат $g(x_1, \dots, x_{n-1}, y_1, \dots, y_k)$ получается из автомата $f(x_1, \dots, x_n)$ подстановкой $h(y_1, \dots, y_k)$ вместо переменной x_n:

$$g(x_1, \dots, x_{n-1}, y_1, \dots, y_k) = \sum_{i=1}^{n-1} u_i(\xi)x_i + u_n(\xi)(\sum_{l=1}^{k} u'_l(\xi)y_l + u'_0(\xi)) + u_0(\xi).$$

Пусть $\Theta \in \{S_{j,s} \mid j \in \mathbb{N},\ s = 1, \dots, 2^{\deg(p_j)}\}$. По определению $\forall v'_1(\xi), \dots, v'_k(\xi) \in \langle r_s(\xi)\rangle_{(p_j)}$, имеем $\langle\left(\sum\limits_{l=1}^{k} u'_l(\xi)v'_l(\xi) + u'_0(\xi)\right)\rangle_{(p_j)} = \langle r_s(\xi)\rangle_{(p_j)}$, следовательно, $\forall v_1(\xi), \dots, v_{n-1}(\xi), v'_1(\xi), \dots, v'_k(\xi) \in \langle r_s(\xi)\rangle_{(p_j)}$ выполнено

$$\sum_{i=1}^{n-1} u_i(\xi)v_i(\xi) + u_n(\xi)(r_s(\xi) + p_j w(\xi)) + u_0(\xi) \in \langle r_s(\xi)\rangle_{(p_j)}.$$

Пусть $\Theta \in \{U_j \mid j \in \mathbb{N}\}$, имеем

$$\sum_{i=1}^{n-1} u_i(\xi) + u_n(\xi)(\sum_{l=1}^{k} u'_l(\xi)) = \sum_{i=1}^{n-1} u_i(\xi) + u_n(\xi)(1 + p_j w(\xi)) \in \langle 1\rangle_{(p_j)}.$$

□

Как следствие одного из результатов работы [6], имеем

Лемма 9. *Пусть $M \subseteq LD_2$. Если $\tilde{S}(M) \cap \tilde{A} \neq \varnothing$, то $\forall\ k \in \mathbb{N}$ автомат*

$$G_k(z, \bar{X}^k, \bar{Y}^k) = z + \xi x_1 + \xi^2 x_2 + \dots + \xi^k x_k + \xi y_1 + \xi^2 y_2 + \dots + \xi^k y_k \in S(M).$$

Докажем четыре вспомогательные леммы.

Лемма 10. *Пусть $M \subseteq LD_2$ и $\tilde{S}(M) \cap \tilde{A} \neq \varnothing$. Если $M \nsubseteq U_j$, то автомат*

$$P_j(x_1) = p_j u_{1,j}(\xi)x_1 + u_{0,j}(\xi) \in S(M).$$

Доказательство. Рассмотрим автомат $f(x_1, \dots x_n) \in M \setminus U_j$. Имеем

$$f'(x_1) = f(x_1, \dots, x_1) = u_1(\xi)x_1 + u_0(\xi),\ u_1(\xi) \notin \langle 1\rangle_{(p_j)}.$$

Если $p_j \mid u_1(\xi)$, то утверждение доказано, иначе имеем $u_1(\xi) \notin \langle 0\rangle_{(p_j)}$ и $u_1(\xi) \notin \langle 1\rangle_{(p_j)}$. Следовательно, существует некоторый многочлен $\tilde{u}(\xi)$, для которого верно

$$\tilde{u}(\xi) \in \langle \xi\,(1+u_1(\xi))\rangle^{-1}_{(p_j)}. \tag{9}$$

Обозначим $\deg(\tilde{u}(\xi)) = k$, тогда найдутся $a_i \in E_2,\ i = 0\ldots k$, для которых

$$\tilde{u}(\xi) = \sum_{i=0}^{k} a_i \xi^i.$$

По лемме 9 автомат

$$G_{k+1}(z, x_1, \ldots, x_{k+1}, y_1, \ldots, y_{k+1}) = z + \xi x_1 + \cdots + \xi^{k+1} x_{k+1} + \\ + \xi y_1 + \cdots + \xi^{k+1} y_{k+1} \in S(M).$$

Рассмотрим подстановку

$$g(x_1) = G_{k+1}(x_1, \sigma_0, \ldots, \sigma_k, x_1, \ldots, x_1),\ \sigma_l = \begin{cases} x_1, & a_l = 0 \\ f'(x_1), & a_l = 1 \end{cases},$$

$$l = 0, \ldots, k\ .$$

имеем

$$g(x_1) = (1 + \xi(1 + u_1(\xi))\tilde{u}(\xi))x_1 + u''_0(\xi) = (1 + u'_1(\xi))x_1 + u''_0(\xi).$$

Из выражения (9) следует, что многочлен $u'_1(\xi) \in \langle 1\rangle_{(p_j)}$, следовательно, $p_j \mid (1 + u'_1(\xi))$. □

Лемма 11. *Пусть $M \subseteq LD_2$ и $\tilde{S}(M) \cap \tilde{A} \neq \varnothing$. Если для некоторого $j \in \mathbb{N}$ выполнено $M \nsubseteq \Theta$, $\forall\, \Theta \in \{U_j\} \cup \{S_{j,s} \mid s = 1, \ldots, 2^{\deg(p_j)}\} \cup \{S_{1,s} \mid s = 1, 2\}$, то $\exists w_j(\xi) \in E_2[\xi]$, для которого автомат*

$$W_j(x_1) = w_j(\xi)x_1,\ w_j(\xi) \notin \langle 1\rangle_{(p_j)}$$

принадлежит $S(M)$.

Доказательство. Покажем, что автоматы

$$\begin{aligned} &d_0(x_1) = p_j \tilde{w}_1(\xi)x_1 + \tilde{w}_0(\xi), \qquad d_1(x_1) = p_j \tilde{w}'_1(\xi)x_1 + \tilde{w}'_0(\xi), \\ &\tilde{w}_0(0) = 0, \qquad \tilde{w}'_0(0) = 1, \qquad \langle \tilde{w}_0(\xi)\rangle_{(p_j)} \neq \langle \tilde{w}'_0(\xi)\rangle_{(p_j)}. \end{aligned} \tag{10}$$

принадлежат $S(M)$. По лемме 10 автомат

$$f(x_1) = p_j u_1(\xi)x_1 + u_0(\xi) \in S(M).$$

Пусть $a = u_0(0)$. Положим $k_1 = 1$, если $a = 0$, и $k_1 = 2$, если $a = 1$. Рассмотрим автомат $f_{k_1}(x_1, \dots, x_n) \in M \setminus S_{1,k_1}$. Имеем

$$f'(x_1) = f_{k_1}(f(x_1), \dots, f(x_1)) = p_j u'_1(\xi) x_1 + u'_0(\xi),\ u'_0(0) \neq a.$$

Если $u'_0(\xi) \notin \langle u_0(\xi)\rangle_{(p_j)}$, то $d_0(x_1), d_1(x_1) \in S(M)$, иначе имеем $\langle u_0(\xi)\rangle_{(p_j)} = \langle u'_0(\xi)\rangle_{(p_j)} = \langle r_{k_2}(\xi)\rangle_{(p_j)}$, для некоторого $r_{k_2}(\xi) \in E_2[\xi]$, $\deg(r_{k_2}(\xi)) < \deg(p_j)$. Рассмотрим автомат $f_{k_2}(x_1, \dots, x_{\bar{n}}) \in M \setminus S_{j,k_2}$ и подстановку

$$f''(x_1) = f_{k_2}(f'(x_1), \dots, f'(x_1)) = p_j u''_1(\xi) x_1 + u''_0(\xi),\ u''_0(\xi) \notin \langle r_{k_2}(\xi)\rangle_{(p_j)}.$$

Далее, в зависимости от значения $u''_0(0)$ одна из пар $f(x_1), f''(x_1)$ или $f'(x_1), f''(x_1)$ реализует автоматы $d_0(x_1), d_1(x_1) \in S(M)$.

Положим $k = \max(\deg(\tilde{w}_0(\xi)), \deg(\tilde{w}'_0(\xi)))$, тогда

$$\tilde{w}_0(\xi) = \sum_{l=0}^{k} a_l \xi^l,\ \tilde{w}'_0(\xi) = \sum_{l=0}^{k} a'_l \xi^l.$$

По лемме 9 автомат

$$G_k(z, \bar{X}^k, \bar{Y}^k) = z + \xi x_1 + \dots + \xi^k x_k + \xi y_1 + \dots + \xi^k y_k \in S(M).$$

Рассмотрим подстановку

$$g(x_1) = G_k(d_0(x_1), \sigma_1, \dots, \sigma_k, \sigma'_1, \dots, \sigma'_k),$$

$$\sigma_l = \begin{cases} x_1, & a_l = 0 \\ d_1(x_1), & a_l = 1 \end{cases}, \qquad \sigma'_l = \begin{cases} x_1, & a'_l = 0 \\ d_0(x_1), & a'_l = 1 \end{cases}, \qquad l = 1, \dots, k.$$

Для некоторого $\bar{u}(\xi) \in E_2[\xi]$ имеем

$$\begin{aligned} g(x_1) &= \left(\tilde{w}_0(\xi) + 1 + \tilde{w}'_0(\xi) + p_j \bar{u}(\xi)\right) x_1 + (\tilde{w}_0(\xi)\tilde{w}'_0(\xi) + \tilde{w}'_0(\xi)\tilde{w}_0(\xi)) = \\ &= \left(1 + \left(\tilde{w}_0(\xi) + \tilde{w}'_0(\xi)\right) + p_j \bar{u}(\xi)\right) x_1. \end{aligned}$$

Из выражения (10) $\langle \tilde{w}_0(\xi)\rangle_{(p_j)} \neq \langle \tilde{w}'_0(\xi)\rangle_{(p_j)}$, следовательно,
$\langle 1 + (\tilde{w}_0(\xi) + \tilde{w}'_0(\xi))\rangle_{(p_j)} \neq \langle 1\rangle_{(p_j)}$. □

Лемма 12. *Пусть $M \subseteq LD_2$ и $\tilde{S}(M) \cap \tilde{A} \neq \varnothing$. Если для некоторого $j \in \mathbb{N}$ выполнено $M \nsubseteq \Theta$, $\forall\ \Theta \in \{U_j\} \cup \{S_{j,s} \mid s = 1, \dots, 2^{\deg(p_j)}\} \cup \{U_1\} \cup \{S_{1,s} \mid s = 1, 2\}$, то $\exists u_j(\xi) \in E_2[\xi]$, $p_j \nmid u_j(\xi)$, такой, что $\forall w(\xi) \in E_2[\xi]$ автомат*

$$f_{j,w(\xi)}(x_1, x_2) = x_1 + \xi w(\xi) u_j(\xi) x_2,$$

принадлежит $S(M)$.

Доказательство. По лемме 9 для любого $k \in \mathbb{N}$ автомат

$$G_k(z, \bar{X}^k, \bar{Y}^k) = z + \xi x_1 + \cdots + \xi^k x_k + \xi y_1 + \cdots + \xi^k y_k \in S(M).$$

По лемме 11 $S(M)$ принадлежит автомат

$$d_j(x_1) = u'_j(\xi)x_1,\ u'_j(\xi) \notin \langle 1 \rangle_{(p_j)}. \tag{11}$$

Пусть $w(\xi) = \sum_{i=0}^{K} a_i \xi^i$, рассмотрим подстановку

$$f_{j,w(\xi)}(x_1, x_2) = G_{K+1}(x_1, \sigma_0, \cdots, \sigma_K, x_2, \cdots, x_2),\ \sigma_i = \begin{cases} x_2, & a_i = 0 \\ d_j(x_2), & a_i = 1 \end{cases},$$

имеем

$$f_{j,w(\xi)}(x_1, x_2) = x_1 + \xi(1 + u'_j(\xi))w(\xi)x_2 = x_1 + \xi w(\xi)u_j(\xi)x_2 \in S(M).$$

Из выражения (11) следует, что $p_j \nmid (1 + u'_j(\xi))$.

$\square$

Лемма 13. *Пусть $M \subseteq LD_2$ и $\tilde{S}(M) \cap \tilde{A} \neq \varnothing$. Если $\exists u_1(\xi) \in E_2[\xi],\ \xi \nmid u_1(\xi)$, такой, что $\forall w(\xi) \in E_2[\xi]$ автомат*

$$f_{1,w(\xi)}(x_1, x_2) = x_1 + \xi w(\xi)u_1(\xi)x_2,$$

принадлежит $S(M)$ и выполнено $M \nsubseteq \Theta,\ \forall\ \Theta \in \{U_j \mid j \in D(u_1(\xi))\} \cup \{S_{j,s} \mid j \in D(u_1(\xi)),\ s = 1, \ldots, 2^{\deg(p_j)}\} \cup \{U_1\} \cup \{S_{1,s} \mid s = 1, 2\}$, то $0 \in S(M)$.

Доказательство. По лемме 12 $\forall j \in D(u_1(\xi))\ \exists u_j(\xi) \in E_2[\xi],\ p_j \nmid u_j(\xi)$, такой, что $\forall w(\xi) \in E_2[\xi]$ автомат

$$f_{j,w(\xi)}(x_1, x_2) = x_1 + \xi w(\xi)u_j(\xi)x_2,$$

принадлежит $S(M)$. Положим $D = \{u_1(\xi)\} \cup D(u_1(\xi)) = \{u_{j_1}(\xi), \cdots, u_{j_S}(\xi)\}$. Имеем НОД$(u_{j_i}(\xi) \mid u_{j_i}(\xi) \in D) = 1$, следовательно, существует набор многочленов $\{v_1(\xi), \cdots, v_S(\xi)\}$ такой, что

$$\sum_{i=1}^{S} v_i(\xi)u_{j_i}(\xi) = 1.$$

По лемме 11 автомат $d(x_1) = \xi u''(\xi)x_1 \in S(M)$. Положим $v_i'(\xi) = u''(\xi)v_i(\xi),\ i = 1, \dots, S$ и рассмотрим

$$f_{j_1,v_1'(\xi)}(f_{j_2,v_2'(\xi)}(\cdots f_{j_S,v_S'(\xi)}(d(x_1),x_1)\cdots,x_1),x_1) =$$
$$= \left(\xi u''(\xi) + \xi u''(\xi)\left(\sum_{i=1}^{S} v_i(\xi)u_{j_i}(\xi)\right)\right)x_1 = 0 \in S(M).$$

$\square$

Докажем основное утверждение раздела. Для произвольного подмножества $M \subseteq LD_2$, покажем, что система $\bar{H} \cup H_0$ является критериальной относительно задачи выразимости константы 0.

Лемма 14. *Пусть* $M \subseteq LD_2$. $0 \in S(M) \iff M \nsubseteq \Theta,\ \forall\ \Theta \in \bar{H} \cup H_0$.

Доказательство. Прямое утверждение следует из того факта, что $\forall\ \Theta \in \bar{H} \cup H_0$ имеем $0 \notin \Theta$ и $S(\Theta) = \Theta$.
Докажем обратное утверждение. По теореме 2 имеем $\tilde{S}(M) \cap \tilde{A} \neq \varnothing$. По лемме 12 $\exists u_1(\xi) \in E_2[\xi],\ p_1 \nmid u_1(\xi)$, такой, что для произвольного $w(\xi) \in E_2[\xi]$ автомат

$$f_{1,w(\xi)}(x_1,x_2) = x_1 + \xi w(\xi)u_1(\xi)x_2,$$

принадлежит $S(M)$. Тогда из леммы 13 следует основное утверждение. $\square$

Лемма 15. *Пусть* $M \subseteq LD_2$, M *— конечное и* $\tilde{S}(M) \cap \tilde{A} \neq \varnothing$. *Проверка условия* $0 \in S(M)$ *алгоритмически разрешима.*

Доказательство. Если $M \nsubseteq \Theta,\ \forall\Theta \in \{U_1, S_{1,1}, S_{1,2}\}$, то по лемме 12 $\exists u_1(\xi) \in E_2[\xi],\ p_1 \nmid u_1(\xi)$, такой, что для произвольного $w(\xi) \in E_2[\xi]$ автомат

$$f_{1,w(\xi)}(x_1,x_2) = x_1 + \xi w(\xi)u_1(\xi)x_2,$$

принадлежит $S(M)$. Положим $D_1 = D(u_1(\xi))$ — множество неприводимых многочленов. По определению имеем $|D_1| < \infty$. Следовательно, если $M \nsubseteq \Theta,\ \forall\ \Theta \in \{U_j \mid j \in D(u_1(\xi))\} \cup \{S_{j,s} \mid j \in D(u_1(\xi)),\ s = 1, \dots, 2^{\deg(p_j)}\} \cup \{U_1\} \cup \{S_{1,s} \mid s = 1, 2\}$, то по лемме 13 имеем $0 \in S(M)$.

Поскольку M конечно, а принадлежность элемента множествам указанного вида проверяется по их определению, то каждое включение $M \subseteq \Theta$ проверяется за конечное число шагов. Следовательно, по ранее доказанному критерию условие $0 \in S(M)$ алгоритмически разрешимо. $\square$

6. Полнота и алгоритмическая разрешимость

Определение 5. Определим семейство подмножеств LD_2:

$$T_j = \{f \mid f \in LD_2,\ f = \sum_{i=1}^{n} u_i(\xi)x_i + u_0(\xi) \text{ и } u_0(\xi) \vdots p_j\},\ j \in \mathbb{N}.$$

Обозначим $H_C = \{T_j\}$.
В работе [10] были доказаны следующие леммы.

Лемма 16. *Пусть $M \subseteq LD_2$, $\tilde{S}(M) \cap \tilde{A} \neq \varnothing$ и автомат $0 \in S(M)$. Если $M \nsubseteq \Theta$, $\forall \Theta \in H_C$, то система M полна в LD_2.*

Лемма 17. *Пусть $M \subseteq LD_2$, M — конечное, $\tilde{S}(M) \cap \tilde{A} \neq \varnothing$ и $0 \in S(M)$. Проверка полноты множества M в LD_2 алгоритмически разрешима.*

Из представленных лемм и доказанных ранее утверждений, напрямую следует основной результат работы.

Теорема 3. *Пусть $M \subseteq LD_2$. Если $M \nsubseteq \Theta$, $\forall \Theta \in \bar{H} \cup H_0 \cup H_C$, то $S(M) = LD_2$.*

Теорема 4. *Пусть $M \subseteq LD_2$, M — конечное. Проверка полноты множества M в LD_2 алгоритмически разрешима.*

7. Заключение

В данной работе был получен критерий полноты для произвольных подмножеств класса линейных дефинитных автоматов. На основании данного критерия был построен алгоритм распознавания полноты произвольных конечных подмножеств рассматриваемого класса. Дальнейшие исследования по теме могут заключаться в обобщении полученных результатов на линейные дефинитные автоматы, построенные над произвольным конечным полем.

В заключение автор выражает особую признательность научному руководителю, д.ф.-м.н. Часовских А. А. за научное руководство, помощь и обсуждение результатов.

Список литературы

[1] П. Кон, *Универсальная алгебра*, М.: Мир, 1968.

[2] В. Б. Кудрявцев, “О мощностях множеств предполных классов некоторых функциональных систем, связанных с автоматами”, *Докл. АН СССР*, **151**:3 (1963), 493–496.

[3] В. Б. Кудрявцев, С. В. Алёшин, А. С. Подколзин, *Введение в теорию автоматов*, М.: Изд-во Московского университета, 2019.

[4] М. И. Кратко, “Алгоритмическая неразрешимость проблемы распознавания полноты для конечных автоматов”, *Докл. АН СССР*, **155**:1 (1964), 35–37.

[5] Д. Н. Жук, “О неразрешимости проблемы полноты для дефинитных автоматов”, *Интеллектуальные системы. Теория и приложения*, **12** (2008), 211–228.

[6] А. А. Часовских, “Проблема полноты в классах линейных автоматов”, *Интеллектуальные системы. Теория и приложения*, **22**:2 (2018), 151–153.

[7] А. А. Часовских, “Об алгоритмической разрешимости проблемы полноты для линейных автоматов”, *Вестник Московского университета. Серия 1. Математика. Механика*, 1986, № 3, 82–84.

[8] А. А. Часовских, “Линейно-автоматные функции с операциями суперпозиции”, *Нейрокомпьютеры: разработка, применение*, 2013, № 8, 3–13.

[9] И. В. Молдованов, “Аппроксимационная полнота линейных дефинитных автоматов”, *Интеллектуальные системы. Теория и приложения*, **29**:4 (2025), 135–149.

[10] И. В. Молдованов, “Алгоритмическая разрешимость задачи полноты конечных содержащих константу ноль множеств в классе линейных дефинитных автоматов”, *Чебышевский сборник*, **26**:5 (2025), 137–157. DOI: 10.22405/2226-8383-2025-26-5-137-157.

[11] А. В. Чашкин, *Лекции по дискретной математике*, М., 2007.

[12] Р. Лидл, Г. Нидеррайтер, *Конечные поля*, **1–2**, М.: Мир, 1988.

[13] Д. Ферран, Ж.-П. Оливье, “Минимальные гомоморфизмы колец”, *Журнал алгебры*, **16**:3 (1970), 461–471. DOI: 10.1016/0021-8693(70)90020-7.

[14] Д. Е. Доббс, Дж. Шапиро, “Классификация минимальных расширений колец целостной области”, *Журнал алгебры*, **305**:1 (2006), 185–193. DOI: 10.1016/j.jalgebra.2005.10.005.

[15] Д. Е. Доббс, Дж. Шапиро, “Классификация минимальных расширений колец некоторых коммутативных колец”, *Журнал алгебры*, **308**:2 (2007), 800–821. DOI: 10.1016/j.jalgebra.2006.07.024.

Статья поступила 26 мая 2026 г.

The completeness problem for linear definite automata

I. V. Moldovanov

This paper studies the completeness problem under superposition in the class of linear definite automata over the finite field with two elements. Its main result is a completeness criterion for arbitrary subsets of linear definite automata, stated in terms of a family of closed classes. This criterion extends earlier results that applied only to finitely generated subsets containing the zero constant. As a consequence, the paper proves that completeness is decidable for finite subsets of the class of linear definite automata.

Keywords: completeness problem, superposition, linear automata, definite automata.

References

[1] P. Cohn, *Universal Algebra*, Moscow: Mir, 1968.

[2] V. B. Kudryavtsev, “On cardinalities of sets of precomplete classes of some functional systems related to automata”, *Dokl. Akad. Nauk SSSR*, **151**:3 (1963), 493–496 (In Russian).

[3] V. B. Kudryavtsev, S. V. Aleshin, A. S. Podkolzin, *Introduction to Automata Theory*, Moscow: MSU Press, 2019.

[4] M. I. Kratko, “Algorithmic unsolvability of the problem of recognizing completeness for finite automata”, *Dokl. Akad. Nauk SSSR*, **155**:1 (1964), 35–37 (In Russian).

[5] D. N. Zhuk, “On the undecidability of the completeness problem for definite automata”, *Intelligent Systems. Theory and Applications*, **12** (2008), 211–228 (In Russian).

[6] A. A. Chasovskikh, “The completeness problem in classes of linear automata”, *Intelligent Systems. Theory and Applications*, **22**:2 (2018), 151–153 (In Russian).

[7] A. A. Chasovskikh, “On algorithmic decidability of the completeness problem for linear automata”, *Moscow University Bulletin. Series 1. Mathematics. Mechanics*, 1986, № 3, 82–84 (In Russian).

[8] A. A. Chasovskikh, “Linear-automata functions with superposition operations”, *Neurocomputers: Development, Application*, 2013, № 8, 3–13 (In Russian).

[9] I. V. Moldovanov, “Approximation completeness of linear definite automata”, *Intelligent Systems. Theory and Applications*, **29**:4 (2025), 135–149 (In Russian).

[10] I. V. Moldovanov, “Algorithmic decidability of the completeness problem for finite sets containing the zero constant in the class of linear definite automata”, *Chebyshevskii Sbornik*, **26**:5 (2025), 137–157. DOI: `10.22405/2226-8383-2025-26-5-137-157` (In Russian).

[11] A. V. Chashkin, *Lectures on Discrete Mathematics*, Moscow, 2007 (In Russian).

[12] R. Lidl, H. Niederreiter, *Finite Fields*, **1–2 (Russian translation)**, Moscow: Mir, 1988.

[13] D. Ferrand, J.-P. Olivier, “Homomorphismes minimaux d’anneaux”, *Journal of Algebra*, **16**:3 (1970), 461–471. DOI: `10.1016/0021-8693(70)90020-7`.

[14] D. E. Dobbs, J. Shapiro, “A classification of the minimal ring extensions of an integral domain”, *Journal of Algebra*, **305**:1 (2006), 185–193. DOI: `10.1016/j.jalgebra.2005.10.005`.

[15] D. E. Dobbs, J. Shapiro, “A classification of the minimal ring extensions of certain commutative rings”, *Journal of Algebra*, **308**:2 (2007), 800–821. DOI: `10.1016/j.jalgebra.2006.07.024`.

Received on May 26, 2026