Классы линейных автоматов над конечными полями с операциями суперпозиции

А. А. Часовских[1]

Для классов линейных автоматов над конечными полями найдены все предполные классы по операциям суперпозиции.

Ключевые слова: конечный автомат, линейный автомат, операции суперпозиции, полнота, предполный класс, конечное поле.

Как известно, конечное поле E_k из k элементов существует, если $k = p^m$ для некоторого простого числа p и натурального числа m [1]. Мы будем использовать понятие линейного автомата над полем E_k из книги [2], и рассматривать только автоматы с одним выходом вместе с операциями суперпозиции [3], которые включают переименование переменных, отождествление переменных и подстановку одного автомата на вход другого автомата. При этом автоматы, отличающиеся только фиктивными входами, мы называем равными, и считаем, что, построив какой-то автомат, мы получаем все равные ему автоматы.

Линейные автоматы над полем E_k получаем замыканием множества, состоящего из сумматора, усилителей и задержек, с использованием операций суперпозиции и обратной связи [4]. Операцию обратной связи в дальнейшем мы не используем. Линейный автомат над полем E_k с n входами является функцией $f(x_1, \ldots, x_n)$, переменные которой принимают значения формальных степенных рядов с коэффициентами из E_k, а значения вычисляются в соответствии с равенством:

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

где μ_i – формальные ряды переменной ξ, коэффициенты которых образуют периодическую (с предпериодом) последовательность и могут быть заданы отношениями многочленов над тем же полем, знаменатели которых имеют ненулевой свободный член.

Класс линейных автоматов над полем E_k с операциями суперпозиции обозначаем LS_k. Мы используем это обозначение и для множества всех линейных автоматов над полем E_k.

[1] *Часовских Анатолий Александрович* — доцент каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: chasovskikh@mail.ru.

Chasovskikh Anatoly Alexandrovich — associate professor, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

Для простых k в классах LS_k в [5] были найдены все максимальные собственные подклассы (предполные классы). Здесь соответствующая задача решена для классов линейных автоматов над полями, не являющимися простыми.

Множество всех линейных автоматов над E_k, сохраняющих элемент a поля E_k в начальный момент времени, обозначаем T_a. Множество всех автоматов из LS_k, значение которых в начальный момент зависит не более чем от одного входа, обозначаем V_1. Автоматы f из LS_k, для которых из (1) следует $\sum_{i=1}^{n} \mu_i(0) = 1$, составляют множество V_k.

Как отмечалось, мы рассматриваем случай $k = p^m$ с $m > 1$. Известно [1], что в этом случае поле E_k содержит максимальные собственные подполя: E_{k_s}, $s = 1, 2, \ldots, l$. Через P_s обозначим множество автоматов из LS_k, все коэффициенты при переменных которых в разложении (1) имеют свободный член из E_{k_s}.

Множество M_1 составляют автоматы из LS_k, значение выхода которых в момент времени, следующий за начальным, не зависят от значений входов в начальный момент. Через M_0 обозначим множество автоматов f, для которых в разложении (1) для каждого коэффициента при переменной степень его числителя не превосходит степени знаменателя. Пронумеруем все неприводимые приведенные многочлены из $E_k[\xi]$ натуральными числами: p_1, p_2, $\ldots$ так, что $p_1 = \xi$. Через M_i обозначим множество всех автоматов f из LS_k, знаменатели коэффициентов при переменных в разложении (1) которых не делятся на p_i, $i = 2, 3, \ldots$.

Теорема 1. *Множество*

$$JS_k = \{\ T_a, V_k, V_1, P_s, M_i \ \mid\ a \in E_k, s \in \{1, \ldots, l\}, i \in \mathbb{Z}_+\}$$

состоит из предполных классов в LS_k, содержит все такие классы и является приведенной S-критериальной системой [3].

Доказательство. Для автомата f с разложением (1) положим: $U(f) = \{\mu_i | i = 1, \ldots, n\}$. Для множества M, $M \subseteq LS_k$, через $U(M)$ обозначим множество $\cup_{f \in M} U(f)$.

Замыкание множества M, $M \subseteq LS_k$, по операциям суперпозиции обозначаем $S(M)$, а замыкание множества M отношений многочленов по операциям сложения и умножения обозначаем $S^{(1)}(M)$. Через $E'_k(\xi)$ мы обозначаем множество всех отношений многочленов переменной ξ с коэффициентами из поля E_k, знаменатели которых имеют ненулевой свободный член.

Замкнутость каждого класса из JS_k доказывается индукцией по операциям суперпозиции. То, что ни один класс из JS_k не содержится в другом, несложно доказать, предъявив для каждого класса Θ из JS_k его подмножество, не содержащееся ни в каком другом классе из JS_k.

Пусть $M \subseteq LS_k$ и для любого Θ, $\Theta \in JS_k$, выполнено: $M \not\subseteq \Theta$. Покажем, что выполнено:

$$S(M) = LS_k. \tag{2}$$

Используя доказательство теоремы 3 из [6], нетрудно показать, что $S^{(1)}(U(M)) = E'_k(\xi)$. Отсюда и из доказательства леммы 2 этой же работы получаем:

$$x_1 + x_2 + \dots + x_{p+1} \in S(M), \tag{3}$$

и для любого μ, $\mu \in E'_k(\xi)$, выполнено:

$$x_0 + \mu x_1 + \mu x_2 + \dots + \mu x_p \in S(M), \tag{4}$$

Из соотношений (3), (4) и $M \setminus V_k \neq \emptyset$ следует, что $S(M)$ содержит автомат с одним входом $g(x) = \mu' x + \mu'_0$, для которого выполнено: $\mu'(0) = 0$. В M входит автомат h, не сохраняющий $\mu'_0(0)$ в начальный момент времени. Тогда для одноместного автомата $g'(x) = h\left(g(x), \dots, g(x)\right)$ имеем: $g'(x) = \mu'' x + \mu''_0,\;\; \mu''(0) = 0,\;\; \mu''_0(0) \neq \mu'_0(0)$.

Из сумматора $x_1 + x_2 + \dots + x_{p+1}$, автоматов $g(x)$ и $g'(x)$, и (при подходящем μ) автомата $x_0 + \mu x_1 + \mu x_2 + \dots + \mu x_p$ с использованием операций суперпозиции строится автомат $\tilde{g}(x) = \tilde{\mu} x + \tilde{\mu}_0$, для которого выполнены равенства: $\tilde{\mu}(0) = 0$, $\tilde{\mu}_0(0) = 0$.

Подставляя вместо всех переменных автомата из M, не сохраняющего 0 в начальный момент времени, автомат $\tilde{g}(x)$, получаем автомат $\tilde{\tilde{g}}(x) = \tilde{\tilde{\mu}} x + \tilde{\tilde{\mu}}_0$, для которого выполнены соотношения: $\tilde{\tilde{\mu}}(0) = 0$, $\tilde{\tilde{\mu}}_0(0) \neq 0$.

Обозначим через r число $\deg\left(\tilde{\mu}_0\right) + \deg\left(\tilde{\tilde{\mu}}_0\right)$. Используя рассуждения из доказательства леммы 3 работы [7], можно показать, что, из множества автоматов

$$\left\{x_0 + a_1\xi x_{1,1} + \dots + a_1\xi x_{1,p} + \dots + a_r\xi^r x_{r,1} + \dots + a_r\xi^r x_{r,p} | a_i \in E_k\right\},$$

которое входит в $S(M)$ ввиду (4), и автоматов $\tilde{g}(x)$, $\tilde{\tilde{g}}(x)$, используя операции суперпозиции, для некоторой дроби $\hat{\mu}$ можно построить автомат $\xi\hat{\mu}x$.

Далее, обобщая доказательство леммы 4 из той же работы, получаем: $0 \in S(M)$. Отсюда и из (3), (4), $\tilde{\tilde{g}}(x) \in S(M)$ получаем (2). Тем самым доказана S-критериальность множества замкнутых классов JS_k [3].

Предполнота каждого класса множества JS_k и отсутствие предполных классов, не содержащихся в JS_k доказываются с использованием известных общих рассуждений [4]. $\square$

Список литературы

[1] Лидл Р., Нидеррайтер Г., *Конечные поля*, «Мир», Москва, 1988, 425 с.

[2] Гилл А., *Линейные последовательностные машины*, «Наука», Москва, 1974, 288 с.

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

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

[5] Часовских А.А., "Классы линейных р-автоматов с операциями суперпозиции", *Интеллектуальные системы. Теория и приложения*, **25**:2 (2021), 155–156

[6] Часовских А.А., "Проблема полноты для класса линейно-автоматных функций", *Дискретная математика*, **27**:2 (2015), 134–151

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

Linear automata classes over finite fields with superposition operations

Chasovskikh A.A.

All precomplete classes are found for classes of linear automata over finite fields with superposition operations.

Keywords: finite automaton, linear automaton, operation of superposition, completeness, maximum subclass, finite field.

References

[1] Lidl R., Niederreiter H., *Finite fields*, «Mir», Moscow, 1988, 425 c.

[2] Gill A., *Linear sequential circuits*, «Science», Moscow, 1974, 288 c.

[3] Kudryavtsev V.B., Alyoshin S.V., Podkolzin A.S., *Introduction to automata theory*, «Science», Moscow, 1985, 320 c.

[4] Chasovskikh A.A., "Maximum subclasses in classes of linear automata over finite fields", *Discrete Math*, **31**:4 (2019), 88–101

[5] Chasovskikh A.A., "Linear p-automata classes with superposition operations", *Intelligent systems*, **25**:2 (2021), 155–156

[6] Chasovskikh A.A., "Completeness problem for the class of linear automata functions", *Discrete Math*, **27**:2 (2015), 134–151

[7] Chasovskikh A.A., "Linear automata functions with superposition operations", *Neurocomputers: development, application*, 2013, №8, 3–13