Проблема A-полноты линейно-автоматных функций над конечным полем

А. А. Часовских

Найдены все *A-предполные подклассы* в классах *линейно-автоматных функций* над конечными полями. Доказана *алгоритмическая разрешимость* проверки *A-полноты* конечных подмножеств в рассматриваемых классах.

Ключевые слова: конечный автомат, линейный автомат, линейно-автоматная функция, оператор A-замыкания, проблема A-полноты, критерий полноты, A-предполный класс, сумматор, задержка.

В работе [5] решена задача A-полноты для класса линейно-автоматных функций (л.-а. функций) над полем $E_2 = \{0, 1\}$. В настоящей работе получено обобщение этого результата для конечно-автоматных функций над конечным полем E_{p^m}, где p — простое, а m — натуральное число.

Зафиксируем простое число p и натуральное число m. Через k обозначим число p^m, а через $E_k[\xi]$ обозначим множество всех многочленов переменной ξ над полем E_k. Для множества всех многочленов из $E_k[\xi]$ с ненулевым свободным членом будем использовать обозначение $E'_k[\xi]$. Поле отношений многочленов из $E_k[\xi]$ обозначаем $E_k(\xi)$, а его подкольцо

$$\left\{ \quad \frac{u(\xi)}{v(\xi)} \quad \middle| \quad u(\xi) \in E_k[\xi], \quad v(\xi) \in E'_k[\xi] \quad \right\}$$

будем обозначать $E'_k(\xi)$. Множество всех формальных рядов переменной ξ с коэффициентами из E_k будем обозначать $R_k(\xi)$.

Пусть n — натуральное число. Отображение $f(x_1, x_2, \ldots, x_n)$ из $R_k^n(\xi)$ в $R_k(\xi)$ называется линейно-автоматной функцией (л.-а. функцией) над E_k, если найдутся $\mu_i, \quad \mu_i \in E'_k(\xi), \quad i = 0, 1, \ldots, n$, такие,

что для любых $\alpha_i, \quad \alpha_i \in R_k(\xi), \quad i = 1, 2, \ldots, n$, выполнено следующее равенство

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

где операции «+» и «·» индуцированы операциями в E_k. Поэтому л.-а. функция $f(x_1, x_2, \ldots, x_n)$ задается выражением $\sum_{i=1}^{n} \mu_i x_i + \mu_0$.

Множество всех л.-а. функций над E_k обозначим $\mathfrak{L}_k$.

Примеры л.-а. функций из $\mathfrak{L}_k$ [3].

- Сумматор от n переменных: $x_1 + x_2 + \cdots + x_n$, $n \in N$.
- Усилители: $a \cdot x$, $a \in E_k \setminus \{0\}$.
- Константы: μ, $\mu \in E_k'(\xi)$.
- Задержка $\xi \cdot x + a$ с начальным состоянием a, $a \in E_k$.

В классе $\mathfrak{L}_k$ рассмотрим оператор замыкания Σ по операциям суперпозиции [1] (стр. 161), а также аппроксимационный оператор замыкания A [2]. Следуя [1] (стр. 179), для ряда $\mu, \quad \mu \in R_k(\xi), \quad \mu = a_0 + a_1\xi + a_2\xi^2 + \ldots, a_i \in E_k, \quad i = 0, 1, \ldots$, и натурального числа τ, через ${}^{\tau}[\mu$ обозначим многочлен $a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{\tau-1}\xi^{\tau-1}$.

Напомним, что для некоторого натурального числа τ две л.-а. функции $f_1(x_1, x_2, \ldots, x_n)$ и $f_2(x_1, x_2, \ldots, x_n)$, называются τ-эквивалентными, если для любых $\alpha_i, \quad \alpha_i \in R_k(\xi), \quad i = 1, 2, \ldots, n$, выполнено:

$${}^{\tau}[f_1(\alpha_1, \alpha_2, \ldots, \alpha_n) =^{\tau} [f_2(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Нетрудно видеть, что τ-эквивалентность л.-а. функций $f_1(x_1, x_2, \ldots, \ldots, x_n)$ и $f_2(x_1, x_2, \ldots, x_n)$, $f_j(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} \mu_{j,i} x_i + \mu_{j,0}$, $j = 1, 2$, равносильно выполнению всех равенств: ${}^{\tau}[\mu_{1,i} =^{\tau} [\mu_{2,i}$, $i = 0, 1, \ldots, n$.

Пусть $M \subseteq \mathfrak{L}_k$. Л.-а. функция f τ-выразима через множество л.-а. функций M, если в $\Sigma(M)$ найдется л.-а. функция g, τ-эквивалентная функции f. Через $\tau(M)$ обозначим множество всех л.-а. функций, τ-выразимых через множество M.

Два множества л.-а. функций M и M' называются τ-эквивалентными, если $\tau(M) = \tau(M')$.

Л.-а. функция $f(x_1, x_2, \ldots, x_n)$ А-выразима через множество M, $M \subseteq \mathfrak{L}_k$, в точности тогда, когда выполнено: $f \in \cap_{\tau=1}^{\infty} \tau(M)$.

Для множества M, $M \subseteq \mathfrak{L}_k$, через $A(M)$ обозначается множество всех л.-а. функций, А-выразимых через M.

Пусть $M \subseteq \mathfrak{L}_k$. Множество M называется А-полным, если $A(M) = \mathfrak{L}_k$. M называется А-замкнутым классом, если выполнено равенство: $M = A(M)$. А-замкнутый класс M называется А-предполным, если $M \neq \mathfrak{L}_k$ и если для любого множества M', $M \subset M' \subseteq \mathfrak{L}_k$, $M' \neq M$, выполнено: $A(M') = \mathfrak{L}_k$.

В настоящей работе найдены все А-предполные классы в $\mathfrak{L}_k$, что позволяет получить алгоритм проверки А-полноты в $\mathfrak{L}_k$ для конечных систем л.-а. функций.

Как нетрудно видеть, л.-а. функции, рассматриваемые в этой работе, в первый момент времени реализуют квазилинейные функции над полем E_k [6], [7]. В работе [7] были определены все замкнутые подклассы в L_k, не содержащиеся в классе одноместных функций. Те из них, которые являются предполными в L_k, а также класс одноместных функций соответствуют рассматриваемым далее замкнутым классам в $\mathfrak{L}_k$ определенным через свойства имеющимся в начальный момент времени у входящих в него функций.

Рассмотрим следующие множества л.-а. функций.

Пусть $s \in E_k$,

$$\begin{aligned} T_s \;=\; \{ \quad & f(x_1, x_2, \ldots, x_n) \quad | \quad n \in N, \quad f \in \mathfrak{L}_k, \quad \text{из} \\ & f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0 \quad \text{следует} \\ & \sum_{i=1}^{n} {}^1[\mu_i \cdot s + {}^1[\mu_0 = s \quad \Big\}. \end{aligned}$$

Таким образом, T_s — множество всех л.-а. функций, сохраняющих число s в начальный момент времени.

Далее, положим

$$\begin{aligned} V_1 \;=\; \{ \quad & f(x_1, x_2, \ldots, x_n) \quad | \quad n \in N, \quad f \in \mathfrak{L}_k, \\ & f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0, \\ & \text{среди чисел} \quad {}^1[\mu_i \,, \quad i = 1, 2, \ldots, n, \\ & \text{не более одного отличного от нуля} \quad \}, \end{aligned}$$

то есть V_1 — множество всех л.-а. функций, зависящих в начальный момент не более чем от одной переменной.

Введем обозначение V_p для множества

$$\left\{ \quad f(x_1, x_2, \ldots, x_n) \quad | \quad n \in N, \quad f \in \mathfrak{L}_k, \quad \text{и из} \right.$$
$$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0 \quad \text{следует}$$
$$\left. \sum_{i=1}^{n} {}^1[\mu_i = 1 \right\}.$$

Пусть $m = q_1^{r_1} \cdot q_2^{r_2} \ldots q_l^{r_l}$ — разложение числа m в произведение простых чисел q_s, $s = 1, 2, \ldots, l$, $q_s \neq q_{s'}$ при $s \neq s'$. Обозначим через k_s число p^{m/q_s}, $s = 1, 2, \ldots, l$.

Для любого s, $s = 1, 2, \ldots, l$, в поле E_k существует единственное подполе E_{k_s}, содержащее k_s элементов, $s = 1, 2, \ldots, l$, [4]. Положим

$$\begin{aligned} P_s \quad = \quad & \{ \quad f(x_1, x_2, \ldots, x_n) \quad | \quad n \in N, \quad f \in \mathfrak{L}_k, \quad \text{из} \\ & f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0 \quad \text{следует} \\ & {}^1[\mu_i \in E_{k_s}, \quad i = 1, 2, \ldots, n \quad \}. \end{aligned}$$

Кроме того, положим

$$\begin{aligned} M(\xi^2) \quad = \quad & \{ \quad f(x_1, x_2, \ldots, x_n) \quad | \quad n \in N, \quad f \in \mathfrak{L}_k, \quad \text{из} \\ & f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0 \quad \text{для любого} \\ & i, \quad i = 1, 2, \ldots, n, \quad \text{следует} \quad \mu_i - {}^1[\mu_i \in \xi^2 E_k'(\xi) \quad \}. \end{aligned}$$

Через AJ_k обозначим следующее множество классов л.-а. функций.

$$\begin{aligned} AJ_k \quad = \quad & \{ \quad V_1, \quad V_p, \quad M(\xi^2), \quad T_s, \quad P_{s'} \quad | \\ & s = 0, 1, \ldots, k-1, \quad s' = 1, 2, \ldots, l \}. \end{aligned}$$

Теорема 1. *Множество AJ_k является приведенной А-критериальной системой А-замкнутых классов в $\mathfrak{L}_k$. То есть справедливы следующие три утверждения:*

- *Для любого* Θ, $\Theta \in AJ_k$, *выполнено:* $A(\Theta) = \Theta$.
- *Для любого* M, $M \subseteq \mathfrak{L}_k$, *равенство* $A(M) = \mathfrak{L}_k$ *выполнено в точности тогда, когда* $M \not\subseteq \Theta$ *для каждого* Θ, $\Theta \in AJ_k$.
- *Для любых* Θ_1, Θ_2 — *различных элементов множества* AJ_k *выполнено:* $\Theta_1 \not\subseteq \Theta_2$.

Теорема 2. *Каждый элемент множества* AJ_k *является A-предполным классом в* $\mathfrak{L}_k$. *A-предполных классов в* $\mathfrak{L}_k$, *не содержащихся в* AJ_k, *не существует.*

Список литературы

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

[2] Буевич В. А. Об алгоритмической неразрешимости распознавания A-полноты для о.-д. функций // Мат. заметки. — М.: Наука, 1972. Вып. 6. — С. 687–697.

[3] Гилл А. Линейные последовательные машины. — М.: Наука, 1974.

[4] Лидл Р., Нидеррайтер Г. Конечные поля. Т. 1. — М.: Мир, 1988. [Пер. изд.: Lidl R., Niederreiter H. Finite fields. — Cambridge University Press, 1984.]

[5] Часовских А. А. О полноте в классе линейных автоматов // Математические вопросы кибернетики. — М.: Наука, 1991. — Вып. 3. — С. 140–166.

[6] Lau D. Function Algebras on Finite Sets. A Basic Course on Many-Valued Logic and Clone Theory. — Rostok: Springer, 2006.

[7] Szendrei Á. On closed classes of quasilinear functions // Chechoslovak Math. J. — Praha: Institute of Mathematics AS CR, 1980. Vol. 30, No 3. — P. 498–509.