Распознавание A-полноты конечных систем линейных автоматов с добавками над кольцом двоично-рациональных чисел

Ронжин Д.В.[1]

Исследуются вопросы A-полноты конечных систем линейных автоматов над кольцом двоично-рациональных чисел. Описано условие полноты конечной системы линейных автоматов, содержащей автомат, реализующий сумматор в первый такт. Доказана алгоритмическая разрешимость задачи определения принадлежности конечного множества линейных автоматов сформулированному набору предполных классов.

Ключевые слова: конечные автоматы, линейные автоматы, двоично-рациональные числа, A-полнота, предполный класс, алгоримическая разрешимость.

1. Введение

Исследование задачи полноты систем конечных автоматов[1] связано с рассмотрением вопроса об A-полноте[2] этих систем. Также часто рассматривается задача полноты систем, содержащих добавки[3]. Интересным для изучения подклассом конечных автоматов являются линейные автоматы[4, 5], для которых описаны условия полноты конечных систем в терминах предполных классов.

Помимо автоматов, функционирующих над конечными алфавитами, интерес представляет исследование линейных автоматов, алфавиты которых являются бесконечными множествами. В работе [6] исследуются вопросы наличия полных систем по операциям композиции и суперпозиции на множестве линейных автоматов, функционирующих над полем рациональных чисел. В работе [7] исследуется сужение указанного класса до

[1] *Ронжин Дмитрий Владимирович* — преподаватель математики в ОАНО "Новая школа e-mail: d.v.ronzhin@gmail.com.

Ronzhin Dmitry Vladimirovich — math teacher at non-profit organization "New School".

автоматов, функционирующих над подкольцом рациональных чисел - множестве двоично-рациональных чисел.

Настоящая работа посвящена дальнейшему исследованию задачи A-полноты линейных автоматов над кольцом двоично-рациональных чисел. Описано условие A-полноты систем, содержащих в качестве добавки автомат, реализующий сумматор в первый такт. Также в настоящей работе доказана алгоритмическая разрешимость задачи распознавания A-полноты конечных множеств линейных автоматов с упомянутой добавкой.

2. Вспомогательные обозначения

Кольцо двоично-рациональных чисел, которое является подкольцом в поле рациональных чисел обозначим через $\mathbb{Q}_{\frac{m}{2^n}}$:

$$\mathbb{Q}_{\frac{m}{2^n}} = \left\{ \frac{m}{2^n} | m \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

Далее в настоящей работе элементы $\mathbb{Q}_{\frac{m}{2^n}}$ рассматриваем в сокращенном виде. $\forall c \in \mathbb{Q}_{\frac{m}{2^n}}, c = \frac{m}{2^n}, \forall k \in \mathbb{Z}$ будем говорить что c кратно k тогда и только тогда, когда m кратно k.

$\forall l, k \in \mathbb{N}$ будем рассматривать конечные автоматы[1] с входным алфавитом $\mathbb{Q}^l_{\frac{m}{2^n}}$, выходным алфавитом $\mathbb{Q}_{\frac{m}{2^n}}$ и алфавитом состояний $\mathbb{Q}^k_{\frac{m}{2^n}}$, функции переходов и выходов являются линейными[4, 5]. Множество всех таких автоматов обозначим $L(\mathbb{Q}_{\frac{m}{2^n}})$[6] и будем называть множеством линейных автоматом над кольцом двоично-рациональных чисел.
Заметим, что множество $L(\mathbb{Q}_{\frac{m}{2^n}})$ имеет конечный базис по операциям композиции[1], а именно:

$$\mathbf{B} = \{V_{\bigoplus}(x, y), V_{\cdot(-\frac{1}{2})}(x), \xi_1(x)\}, \text{ где}$$

1) $V_{\bigoplus}(x, y)$ - сумматор,

2) $V_{\cdot(-\frac{1}{2})}(x)$ - умножитель на чило $-\frac{1}{2}$,

3) $\xi_1(x)$ - задежрка с единичным начальным состоянием.

Аналогично[7] определим множество формальных степенных рядов над $\mathbb{Q}_{\frac{m}{2^n}}$:

$$\mathbb{Q}^{\infty}_{\frac{m}{2^n}}(\xi) = \left\{ \alpha = \sum_{i=0}^{\infty} a_i \cdot \xi^i \mid a_i \in \mathbb{Q}_{\frac{m}{2^n}} \right\}$$

Сложение и умножение элементов из $\mathbb{Q}^{\infty}_{\frac{m}{2^n}}(\xi)$ определется естественным образом. Автомат из $L(\mathbb{Q}_{\frac{m}{2^n}})$ с l входами будем рассматривать как отображение из $\mathbb{Q}^{\infty}_{\frac{m}{2^n}}(\xi)^l$ в $\mathbb{Q}^{\infty}_{\frac{m}{2^n}}(\xi)$.

Через $\gcd(x, y)$ будем обозначать наибольший общий делитель элементов x, y. Для элементов $\mathbb{Q}_{\frac{m}{2^n}}$ НОД определяется как НОД числителей. Обозначим множество дробно-рациональных функций от переменной ξ с коэффициентами из $\mathbb{Q}_{\frac{m}{2^n}}$ следующим образом[7]:

$$\mathbf{R}(\mathbb{Q}_{\frac{m}{2^n}}) = \left\{ \frac{P(\xi)}{Q(\xi)} \mid P(\xi), Q(\xi) \in \mathbb{Q}_{\frac{m}{2^n}}[\xi], Q(0) = 1, \gcd\left(P(\xi),\ Q(\xi)\right) = 1 \right\}$$

Можно заметить, что $\mathbf{R}(\mathbb{Q}_{\frac{m}{2^n}})$ является подкольцом в кольце $\mathbb{Q}^{\infty}_{\frac{m}{2^n}}(\xi)$.

Доказательство следующих лемм аналогично приведенным в [7]:

Лемма 1. $\forall V(x_1, ..., x_l) \in L(\mathbb{Q}_{\frac{m}{2^n}}), \exists R_0, R_1, ..., R_l \in \boldsymbol{R}(\mathbb{Q}_{\frac{m}{2^n}})$, *такие что:*

$$V(x_1, ..., x_l) = R_0 + \textstyle\sum_{i=1}^{l} R_i \cdot x_i.$$

Лемма 2. $\forall V(x_1, ..., x_l) \colon (\mathbb{Q}^{\infty}_{\frac{m}{2^n}})^l \ \to \mathbb{Q}^{\infty}_{\frac{m}{2^n}}$, *такого что:*

$$V(x_1, ..., x_l) = R_0 + \textstyle\sum_{i=1}^{l} R_i \cdot x_i$$
$$, R_i \in \boldsymbol{R}(\mathbb{Q}_{\frac{m}{2^n}}), i \in [0, l]$$

верно, что $V(x_1, ..., x_l) \in L(\mathbb{Q}_{\frac{m}{2^n}})$.

Множители R_k будем называть коэффициентами отображения. Через $R_k[t]$ будем обозначать t-й член последовательности R_k.

Рассматривается задача A-полноты[2] системы линейных автоматов в $L(\mathbb{Q}_{\frac{m}{2^n}})$. A - замыкание системы M будем обозначать через $A(M)$, замыкание системы M по операциям композиции через $K(M)$, замыкание по операциям суперпозиции через $\Sigma(M)$. Множество линейных автоматов M будет называться A-полным, если $\forall V \in L(\mathbb{Q}_{\frac{m}{2^n}})$ и $\forall \tau \in \mathbb{N}$, в $K(M)$ существует автомат V', совпадающий с автоматом V на словах длины τ.

Ранее был сформулирован ряд K-замкнутых классов, а так же доказана их A-предполнота[7]:

1) Зафиксируем число $k \in \mathbb{N}$ и множество

$$\mathbf{P} = \{p_i | p_i \neq 2 \text{ - простое число}, i \in [1, k]\}.$$

Будем говорить, что автомат $V \in L(\mathbb{Q}_{\frac{m}{2^n}})$, такой что:

$$V(x_1,..,x_l) = R_0 + \sum_{i=1}^{l} R_i \cdot x_i,$$
$$\forall i \in [0,l], R_i \in \mathbf{R}(\mathbb{Q}_{\frac{m}{2^n}}),\ |\{R_j | R_j[0] \neq 0, j \in [1,l]\}| = l',$$

обладает **P**-свойством, если с точностью до переименования входов автомата V выполнено хотя бы одно из следующих условий:

а) $l' \leq 1$.

б) $\exists i \in [1,k] : R_j[0] \vdots p_i, \forall j \in [1,l]$.

в) $R_j[0] \vdots p_1 \cdot p_2 \cdot ... \cdot p_k, \forall j \in [2,l]$.

Определим множество $V_{\mathbf{P}}$ следующим образом:

$$V_{\mathbf{P}} = \{V\ | V \in L(\mathbb{Q}_{\frac{m}{2^n}}), V- \text{ обладает } \mathbf{P}\text{-свойством }\}.$$

2) Будем говорить, что автомат $V(x_1,...,x_l) \in L(\mathbb{Q}_{\frac{m}{2^n}})$, который реализует отображение:

$$V(x_1,..,x_l) = R_0 + \sum_{i=1}^{l} R_i \cdot x_i,$$
$$\forall i \in [0,l], R_i \in \mathbf{R}(\mathbb{Q}_{\frac{m}{2^n}}),\ |\{R_j | R_j[0] \neq 0, j \in [1,l]\}| = l',$$

обладает **D**-свойством, если с точностью до переименования входов автомата V выполнено хотя бы одно из следующих условий:

а) $l' \leq 1$.

б) $\exists p > 2$ - простое : $R_i[0] \vdots p, \forall i \in [1,l]$.

Определим класс D следующим образом:

$$D = \{V\ | V \in L(\mathbb{Q}_{\frac{m}{2^n}}), V- \text{ обладает } \mathbf{D}\text{-свойством }\}.$$

3) $\forall p > 2$, где p - простое число, определим класс M_p следующим образом:

$$M_p = \{V(x_1,..,x_l) \in L(\mathbb{Q}_{\frac{m}{2^n}}) | V(x_1,..,x_l) =$$
$$R_0(\xi) + \sum_{i=1}^{l} R_i(\xi) \cdot x_i, R_i[1] \vdots p, \forall i \in [1,l]\}.$$

4) $\forall p > 2$, где p - простое число, определим класс T_p следующим образом:

$$T_p = \left\{V(x_1,..,x_l) \in L(\mathbb{Q}_{\frac{m}{2^n}}) | V(x_1,..,x_l) = R_0(\xi) + \sum_{i=1}^{l} R_i(\xi)\cdot x_i, R_0[0] \vdots p\right\}.$$

5) Определим класс T_{int} следующим образом:

$$T_{int} = \{V(x_1,..,x_l) \in L(\mathbb{Q}_{\frac{m}{2^n}}) | V(x_1,..,x_l) = R_0(\xi) + \sum_{i=1}^{l} R_i(\xi)\cdot x_i, R_i[0] \in \mathbb{Z}, \forall i \in [1,l]\}.$$

6) Определим класс $T_{\geq 0}$ следующим образом:

$$T_{\geq 0} = \{V(x_1,..,x_l) \in L(\mathbb{Q}_{\frac{m}{2^n}}) | V(x_1,..,x_l) = R_0(\xi) + \sum_{i=1}^{l} R_i(\xi)\cdot x_i, R_i[0] \geq 0, \forall i \in [1,l]\}.$$

Далее в настоящей работе без ограничения общности не будем различать автоматы из $L(\mathbb{Q}_{\frac{m}{2^n}})$ и отображения, которые они реализуют.

3. Основные результаты

Теорема 1. *Пусть $M \subset L(\mathbb{Q}_{\frac{m}{2^n}})$ - конечная система, причем:*

$$f^{(1)}_{\oplus}(x,y) \in M, \text{ где } f^{(1)}_{\oplus}(x,y) = R_1\cdot x + R_2\cdot y + R_0,$$
$$R_1[0] = R_2[0] = 1, R_0[0] = 0.$$

$$A(M) = L(\mathbb{Q}_{\frac{m}{2^n}}) \iff \forall p > 2 \text{ - простого, } M \not\subseteq T_p, M_p, T_{int}, T_{\geq 0}.$$

Доказательство. Импликация

$$A(M) = L(\mathbb{Q}_{\frac{m}{2^n}}) \Rightarrow \forall p > 2 \text{ - простого, } M \not\subseteq T_p, M_p, T_{int}, T_{\geq 0}$$

верна, поскольку классы $T_p, M_p, T_{int}, T_{\geq 0}$ являются A-предполными. Докажем обратную импликацию. Поскольку верно, что $A(M \cup \{V_{\oplus}(x,y)\}) = L(\mathbb{Q}_{\frac{m}{2^n}})$[7], нам достаточно показать что $V_{\oplus}(x,y) \in A(M)$.

1) Покажем, что $\forall g(x_1,x_2,..,x_n) \in L$, где L - линейные функции над кольцом двоично-рациональных чисел, $\exists f(x_1,x_2,..,x_n) \in A(M)$ - линейный автомат, реализующий g в первый такт.

   Заметим, что $\forall n \in \mathbb{N}, n \geq 2$:

$$f_{\cdot n}(x) = \underbrace{f^{(1)}_{\oplus}(x, f^{(1)}_{\oplus}(x, f(.., f^{(1)}_{\oplus}(x,x)..))}_{n-1} = R'_1\cdot x + R'_0,\ R'_1[0] = n,$$
$$R'_0[0] = 0.$$

Поскольку $M \not\subseteq T_{\geq 0}$, без ограничения общности $\exists f_{(<0)}(x,y) \in M$, что:

$$f_{(<0)}(x,y) = R_1'' \cdot x + R_2'' \cdot y + R_0'',\ R_1''[0] < 0.$$

$\exists m \in \mathbb{N}, m > 0, m \cdot R_1''(0) \in \mathbb{Z}$. Следовательно:

$$f_{\cdot m}(f_{(<0)}(x,y)) = R_1^{(3)} \cdot x + R_2^{(3)} \cdot y + R_0^{(3)},\ R_1^{(3)}[0] < 0, R_1^{(3)}[0] \in \mathbb{Z}.$$

$\exists k \in \mathbb{N}$, такое что:

$$f_{(<0)}^{(1)}(x,y) = \underbrace{f_{\bigoplus}^{(1)}(x,..,f_{\bigoplus}^{(1)}(x,f_{\cdot m}(f_{(<0)}(x,y))))}_{k} = R_1^{(4)}\cdot x + R_2^{(4)}\cdot y + R_0^{(4)},$$
$$R_1^{(4)}[0] = -1,$$
$$f_{(<0)}^{(2)}(x,y) = \underbrace{f_{\bigoplus}^{(1)}(x,..,f_{\bigoplus}^{(1)}(x,f_{\cdot m}(f_{(<0)}(x,y))))}_{k+1} = R_1^{(5)}\cdot x + R_2^{(5)}\cdot y + R_0^{(5)},$$
$$R_1^{(5)}[0] = 0, R_2^{(5)}[0] = R_2^{(4)}[0], R_0^{(5)}[0] = R_0^{(4)}[0].$$

Получим автоматы, реализующие в первый такт умножители на 0 и -1:

$$f_{.0}^{(1)}(x) = f_{(<0)}^{(1)}(f_{(<0)}^{(2)}(x,x),x) = R_1^{(6)} \cdot x + R_0^{(6)}, R_1^{(6)}[0] = R_0^{(6)}[0] = 0,$$
$$f_{.(-1)}^{(1)}(x) = f_{(<0)}^{(1)}(f_{\bigoplus}^{(1)}(x, f_{(<0)}^{(2)}(x,x)),x) = R_1^{(7)} \cdot x + R_0^{(7)},$$
$$R_1^{(7)}[0] = -1, R_0^{(7)}[0] = 0.$$

Поскольку $M \not\subseteq T_{int}$, без ограничения общности,$\exists f_{\notin\mathbb{Z}}^{(1)}(x,y) \in M$, что:

$$f_{\notin\mathbb{Z}}^{(1)}(x,y) = R_1^{(8)} \cdot x + R_2^{(8)} \cdot y + R_0^{(8)},\ R_1^{(8)}[0] \notin \mathbb{Z}.$$

Получим автомат, реализующий в первый такт умножитель на $\frac{1}{2}$:

$$f_{\notin\mathbb{Z}}^{(2)}(x) = f_{\bigoplus}^{(1)}(f_{\notin\mathbb{Z}}^{(1)}(x, f_{.0}^{(1)}(x)), f_{.(-1)}^{(1)}(f_{\notin\mathbb{Z}}^{(1)}(f_{.0}^{(1)}(x), f_{.0}^{(1)}(x)))) =$$
$$R_1^{(9)} \cdot x + R_0^{(9)},\ R_1^{(9)}[0] = \frac{m}{2^n} \notin \mathbb{Z}, R_0^{(9)}[0] = 0, m \in \mathbb{Z}, n \in \mathbb{N}.$$

Т.к. уже получен автомат $f_{.(-1)}^{(1)}(x)$, без ограничения общности будем считать $m < 0$. Так как $\exists k \in \mathbb{Z}, k \geq 0$, такое что $k + \frac{m}{2} = \frac{1}{2}$, получим искомый автомат:

$$f^{(1)}_{\cdot(\frac{1}{2})}(x) = \underbrace{f^{(1)}_{\bigoplus}(x, f^{(1)}_{\bigoplus}(x, .., f^{(1)}_{\bigoplus}(x, f^{(1)}_{\cdot(2^{n-1})}(f^{(2)}_{\notin\mathbb{Z}}(x))))}_{k-1} = R^{(10)}_1 \cdot x + R^{(10)}_0,$$
$$R^{(10)}_1[0] = \tfrac{1}{2}, R^{(10)}_0[0] = 0.$$

Для завершения первого шага, необходимо получить константу 1 в первый такт - таким образом будет получен базис линейных функций в кольце двоично-рациональных чисел. В силу конечности M, перенумеруем элементы этого множества:

$$M = \{f_i(x_1, .., x_k) | i \in [1, r]\}.$$

Рассмотрим следующее множество линейных автоматов:

$$S = \{h_i(x) | h_i(x) = f_i(f^{(1)}_{\cdot 0}(x), ..., f^{(1)}_{\cdot 0}(x)), \forall i \in [1, r]\}.$$

Используя автоматы $f^{(1)}_{\cdot 2^n}, \forall n \in \mathbb{N}$, можем добиться выполнения следующего условия:

$$\forall h_i(x) \in S : h_i(x) = R^i_1 \cdot x + R^i_0, R^i_1[0] = 0, R^i_0[0] \in \mathbb{Z}.$$

Поскольку $\forall p > 2$ - простого, $M \not\subseteq T_p$, верно:

$$\exists l \in \mathbb{N} \cup \{0\} : \gcd(R^1_0[0], R^2_0[0], ..., R^r_0[0]) = 2^l.$$

Таким образом, используя полученные ранее $f^{(1)}_{\cdot(-1)}(x), f^{(1)}_{\cdot(n)}(x) \forall n \in \mathbb{N}$, $f^{(1)}_{\cdot(\frac{1}{2})}(x)$, и автомат $f^{(1)}_{\bigoplus}(x, y)$, расширенным алгоритмом Евклида получим автомат, реализующий константу 1 в первый такт.

2) Введем новые обозначения для полученных на предыдущем этапе автоматов:

- $f^{(1)}_{\bigoplus}(x, y) = R^{(1)}_1 \cdot x + R^{(1)}_2 \cdot y + R^{(1)}_0; R^{(1)}_1[0] = R^{(1)}_2[0] = 1, R^{(1)}_0[0] = 0,$
- $f^{(1)}_{\cdot(-1)}(x) = R^{(2)}_1 \cdot x + R^{(2)}_0; R^{(2)}_1[0] = -1, R^{(2)}_0[0] = 0.$

Покажем, что без ограничения общности можем утверждать следующее:

- $S_R = \{R^{(1)}_1[1], R^{(1)}_2[1], R^{(2)}_1[1]\} \subset \mathbb{Z},$

- Либо $S_R = \{0\}$, либо $S_R = \{1, -1\}$, либо $\exists \mathbf{P} = \{p_1, p_2, ..., p_k\}, \forall i \in [1, k], \exists \alpha_i \in \mathbb{N}, \forall c \in S_R : c = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$.

Поскольку $\underbrace{f_{\cdot 0}^{(1)}(f_{\cdot 0}^{(1)}(...(f_{\cdot 0}^{(1)}(x)))}_{n}$ моделирует константу до такта n, очевидно что $\exists \gamma \in A(M)$, $\gamma[0] = 0$, γ - константный автомат.

Построим из $f_{\bigoplus}^{(1)}(x, y)$ следующий автомат:

$$h_{\bigoplus}(x, y) = f_{\bigoplus}^{(1)}(f_{\bigoplus}^{(1)}(\gamma, x), f_{\bigoplus}^{(1)}(y, \gamma)) = R'_1 \cdot x + R'_2 \cdot y + R'_0, \text{ где:}$$
$$R'_1[0] = R'_2[0] = 1, R'_0[0] = 0, R'_1[1] = R'_2[1] = c = \frac{m}{2^n}.$$

В случае, если $c \in \mathbb{Z}$ указанные ограничения для $h_{\bigoplus}(x, y)$ выполняются. В противном случае, рассмотрим следующую подстановку:

$$h_{\bigoplus}(\underbrace{h_{\bigoplus}(...h_{\bigoplus}(x, \gamma), \gamma), \gamma)}_{2^n - 1}, \underbrace{h_{\bigoplus}(...h_{\bigoplus}(y, \gamma), \gamma), \gamma))}_{2^n - 1} =$$
$$R''_1 \cdot x + R''_2 \cdot y + R''_0.$$

Примем за множество $\mathbf{P}$ различные простые делители $R''_1[1]$. Заметим, что для R''_1 и R''_2 указанные выше ограничения выполняются. Без ограничения общности будем называть этот автомат $f_{\bigoplus}^{(1)}(x, y)$.

Рассмотрим $f_{\cdot(-1)}^{(1)}(x)$ и применим следующую подстановку:

$$\hat{h}(x) = f_{\bigoplus}^{(1)}(f_{\cdot(-1)}^{(1)}(f_{\cdot(-1)}^{(1)}(x)), f_{\cdot(-1)}^{(1)}(x)),$$
$$h_{\cdot(-1)}^{(1)}(x) = f_{\bigoplus}^{(1)}(\hat{h}(x), f_{\cdot(-1)}^{(1)}(x)) = \hat{R}_1 \cdot x + \hat{R}_0, \text{ где}$$
$$\hat{R}_1[0] = -1, \hat{R}_1[1] = -R_1^{(1)}[1], \hat{R}_0[0] = 0.$$

Для полученного автомата $h_{\cdot(-1)}^{(1)}(x)$ указанные ограничения выполнены, без ограничения общности будем называть этот автомат $f_{\cdot(-1)}^{(1)}(x)$.

На предыдущем этапе был получен автомат $f_{\cdot(\frac{1}{2})}^{1}(x) = R_1^{(3)} \cdot x + R_0^{(3)}$, где $R_1^{(3)}[0] = \frac{1}{2}, R_0^{(3)}[0] = 0$. Покажем, что без ограничения общности можем считать $R_1^{(3)}[1] = 0$, рассмотрев следующую цепочку преобразований:

$$h_1(x) = f^{(1)}_{\cdot(-1)}(f^{(1)}_{\bigoplus}(f^1_{\cdot(\frac{1}{2})}(x), f^1_{\cdot(\frac{1}{2})}(x))),$$
$$h_2(x) = f^{(1)}_{\bigoplus}(f^1_{\cdot(\frac{1}{2})}(x), f^1_{\cdot(\frac{1}{2})}(h_1(x))),$$
$$h_3(x) = f^{(1)}_{\bigoplus}(f^{(1)}_{\bigoplus}(f^1_{\cdot(\frac{1}{2})}(x), h_2(x)), \gamma).$$

Непосредственной проверкой можно убедиться, что $h_3(x)$ удовлетворяет указанному условию для $f^{(1)}_{\cdot(\frac{1}{2})}(x)$, будем без ограничения общности называть его $f^{(1)}_{\cdot(\frac{1}{2})}(x)$.

3) Получим следующий линейный автомат:

$f^{(1)}_{\xi}(x) = R^{(4)}_1 \cdot x + R^{(4)}_0$, где $R^{(4)}_1[0] = 0, R^{(4)}_1[1] = 1, R^{(4)}_0[0] = 0$.

Используя обозначения из предыдущего пункта имеем одну из следующих альтернатив:

- $|\mathbf{P}| = 0$, если $S_R = \{1, -1\}$,
- $|\mathbf{P}| = \infty$, если $S_R = \{0\}$,
- $\mathbf{P} = \{p_1, p_2, ..., p_k\}, \forall i \in [1, k], \exists \alpha_i \in \mathbb{N}, \forall c \in S_R : c = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$.

Разберем эти случаи:

а) $\mathbf{P} = \emptyset$.

Тогда возможен один из двух вариантов:

- $R^{(1)}_1[1] = R^{(1)}_2[1] = 1, R^{(2)}_1[1] = -1$.
  Тогда искомый автомат получается следующей подстановкой:
  $$f^{(1)}_{\xi}(x) = f^{(1)}_{\cdot(-1)}(f^{(1)}_{\bigoplus}(x, f^{(1)}_{\cdot(-1)}(x))).$$
- $R^{(1)}_1[1] = R^{(1)}_2[1] = -1, R^{(2)}_1[1] = 1$.
  Тогда искомый автомат получается следующей подстановкой:
  $$f^{(1)}_{\xi}(x) = f^{(1)}_{\bigoplus}(x, f^{(1)}_{\cdot(-1)}(x)).$$

б) $|\mathbf{P}| = \infty$.

В таком случае $R^{(1)}_1[1] = R^{(1)}_2[1] = R^{(2)}_1[1] = 0$. Нетрудно заметить, что тогда уже получены сумматор в первые два такта и умножители на все целые числа в первые два такта с точностью до констатного слагаемого.

Поскольку $M \not\subseteq M_p, \forall p > 2$ - простых, выделим подмножество $M' \subseteq \Sigma(M)$, которое, в силу наличия умножителей, сумматора на два такта и константы γ, будет иметь вид:

$$M' = \{f_i(x) = R_i \cdot x + R_0 | f_i(x) = f'_i(x, \gamma, .., \gamma) \in M, \\ R_i[0], R_i[1] \in \mathbb{Z}, \forall i \in [1, r]\}, \text{ причем} \\ \exists l \in \mathbb{N} \cup \{0\} : \gcd(R_1[1], R_2[1], ..., R_r[1]) = 2^l.$$

Используя расширенный алгоритм Евклида и автоматы из M' несложно получить линейный автомат:

$$g(x) = R_1 \cdot x + R_0, \text{ где } R_1[1] = 2^l.$$

Заметим, что подстановкой автомата $f^{(1)}_{\cdot(\frac{1}{2})}(x)$ в себя l раз получаем автомат $f^{(1)}_{\cdot(\frac{1}{2^l})}(x)$, который реализует умножитель на $\frac{1}{2^l}$ в первый такт, и пропускает второй такт. Тогда:

$$f^{(1)}_{\xi}(x) = f^{(1)}_{\cdot(\frac{1}{2^l})}(f^{(1)}_{\bigoplus}(g(x), f^{(1)}_{\cdot(-R_1[0])}(x)))$$

в) $0 < |\mathbf{P}| < \infty$.

Покажем, что $\forall p \in \mathbf{P}, \exists f_p(x) \in A(M)$:

$f_p(x) = R \cdot x + R_0, R[0] = 0, R[1] \in \mathbb{Z}$, причем $R[1]$ не кратно p.

Поскольку $\forall p \in \mathbf{P}, M \notin M_p$, а также поскольку $f_{\cdot 2^n}(x), \gamma \in A(M)$, $\exists f'_p(x) \in A(M)$, такое что $f'_p(x) = R' \cdot x + R'_0$, $R'[1] \in \mathbb{Z}$, причем $R'[1]$ не кратно p. Тогда:

$$f_p(x) = f^{(1)}_{\bigoplus}(f'_p(x), f_{\cdot(-R'[0])}(x))$$

Заметим, что

$$h(x) = f^{(1)}_{\bigoplus}(f^{(1)}_{\cdot(-1)}(x), x) = R \cdot x + R_0, \text{ где} \\ R_0[0] = R[0] = 0,$$

причем $\exists \alpha_1, \alpha_2, ..., \alpha_k \in \mathbb{N}$, такие что $R[1] = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$. Рассмотрим множество линейных автоматов $\{h(x), f_p(x) | p \in \mathbf{P}\}$. Поскольку коэффициенты при переменной x у элементов данного множества равны нулю в первый такт и в совокупности взаимнопросты во второй такт, используя расширенный алгоритм Евклида и полученные ранее автоматы $f^{(1)}_{\bigoplus}(x, y)$ и $f^{(1)}_{\cdot c}(x), \forall c \in \mathbb{Z}$, получим искомый $f^{(1)}_{\xi}(x)$.

Заметим, что для автомата $f^{(1)}_{\xi}(x)$ без ограничения общности можно считать $R^{(4)}_0[1] = 0$, рассмотрев подстановку:

$$f^{(1)}_{\bigoplus}(f^{(1)}_{\xi}(x), f^{(1)}_{\xi}(h(x))), \text{ где}$$
$$h(x) = R \cdot x + R_0 \in A(M),$$
$$R[0] = 0, R_0[0] = -2 \cdot R^{(4)}_0[1] - R^{(1)}_0[1].$$

4) Индукцией по номеру такта покажем что $V_{\bigoplus}(x, y) = x + y \in A(M)$.

База индукции: автомат $f^{(1)}_{\bigoplus}(x, y)$ моделирует сумматор в первый такт, автомат $f^{(1)}_{\xi}(x)$ - моделирует задержку в первый и второй такты.

Переход: Пусть до такта $\tau \geq 1$ автомат $f^{(\tau)}_{\bigoplus}(x, y) = R^{(\tau)}_1 \cdot x + R^{(\tau)}_2 \cdot y + R^{(\tau)}_{0,1}$ моделирует сумматор, а автомат $f^{(\tau)}_{\xi}(x) = R^{(\tau)}_3 \cdot x + R^{(\tau)}_{0,2}$ моделирует задержку. Сначала построим автомат $f^{(\tau+1)}_{\xi}(x)$ - автомат, моделирующий задержку до такта $\tau + 1$. Для этого, используя автоматы $f^{(1)}_{\bigoplus}(x, y), f^{(1)}_{\cdot c}(x), \forall c \in \mathbb{Z}, f^{(1)}_{\cdot \frac{1}{2}}(x)$ и константный автомат γ, построим вспомогательный автомат:

$$\hat{f}^{(1)}(x) = R'_1 \cdot x + R'_0,$$
$$R'_1[0] = -R^{(\tau)}_3[\tau + 1], R'_0[0] = -R^{(\tau)}_{0,1}[\tau + 1] - R^{(\tau)}_{0,2}[\tau + 1].$$

Тогда:

$$f^{(\tau+1)}_{\xi}(x) = f^{(\tau)}_{\bigoplus}(f^{(\tau)}_{\xi}(x), f^{(\tau)}_{\xi}(f^{(1)}_{\xi}(\hat{f}^{(1)}(x)))).$$

Построим автомат $f^{(\tau+1)}_{\bigoplus}(x, y)$. Автомат $f^{(\tau)}_{\bigoplus}(x, f^{(\tau)}_{\bigoplus}(y, z))$ моделирует сумматор из трёх элементов. Обозначим его:

$$f^{(\tau)}_{\bigoplus}(x, y, z) = R^{(\tau)}_1 \cdot x + R^{(\tau)}_2 \cdot y + R^{(\tau)}_3 \cdot z + R^{(\tau)}_0.$$

Используя автоматы $f^{(1)}_{\bigoplus}(x, y), f^{(1)}_{\cdot c}(x), \forall c \in \mathbb{Z}, f^{(1)}_{\cdot \frac{1}{2}}(x)$, построим вспомогательный автомат:

$$f^{(1)}(x, y) = R'_1 \cdot x + R'_2 \cdot y + R'_0,$$
$$R'_1[0] = 1 - R^{(\tau)}_1[\tau + 1], R'_2[0] = 1 - R^{(\tau)}_2[\tau + 1], R'_0[0] = -R^{(\tau)}_0[\tau + 1].$$

В таком случае, искомый автомат выражается следующим образом:

$$f^{(\tau+1)}_{\bigoplus}(x, y) = f^{(\tau)}_{\bigoplus}(x, y, f^{(\tau+1)}_{\xi}(f^{(1)}(x, y))).$$

□

Рассмотрим теперь задачу распознавания принадлежности конечного множества линейных автоматов сформулированным ранее A-предполным классам. Введем обозначения:

$$\forall V \in L(\mathbb{Q}_{\frac{m}{2^n}}),$$
$$U(V) = \{R_i \in \mathbf{R}(\mathbb{Q}_{\frac{m}{2^n}}) | V(x_1, ..., x_l) = R_0 + R_1 \cdot x_1 + R_2 \cdot x_2 + ... + R_l \cdot x_l\}.$$

$$\forall M \subset L(\mathbb{Q}_{\frac{m}{2^n}}),$$
$$U(M) = \{R_i \in \mathbf{R}(\mathbb{Q}_{\frac{m}{2^n}}) | \exists V \in M : R_i \in U(V)\},$$
$$U_t(M) = \{R_i[t] | R_i \in U(M)\}, \forall t \in \mathbb{N} \cup \{0\}.$$

Пользуясь обозначениями, введенными ранее:

$$\mathbf{R}(\mathbb{Q}_{\frac{m}{2^n}}) = \left\{ \frac{P(\xi)}{Q(\xi)} \mid P(\xi), Q(\xi) \in \mathbb{Q}_{\frac{m}{2^n}}[\xi], Q(0) = 1, \gcd\left(P(\xi),\ Q(\xi)\right) = 1 \right\}.$$

Через max обозначим функцию максимума, определенную на $\mathbb{Q}_{\frac{m}{2^n}}$. Через $\deg(P(\xi))$ обозначим степень многочлена $P(\xi)$. Введем вспомогательные определения:

$$\forall R = \frac{P(\xi)}{Q(\xi)} \in \mathbf{R}(\mathbb{Q}_{\frac{m}{2^n}}),$$
$$\deg(R) = \max(\deg(P(\xi)), \deg(Q(\xi))).$$

$$\forall V \in L(\mathbb{Q}_{\frac{m}{2^n}}), V(x_1, ..., x_l) = R_0 + R_1 \cdot x_1 + R_2 \cdot x_2 + ... + R_l \cdot x_l,$$
$$\deg(V) = \max(\deg(R_0), \deg(R_1), \deg(R_2), ..., \deg(R_l)).$$

$$\forall M \subset L(\mathbb{Q}_{\frac{m}{2^n}}), M = \{V_1, V_2, ..., V_n\},$$
$$\deg(M) = \max(\deg(V_1), \deg(V_2), ..., \deg(V_n)).$$

Зафиксируем конечную систему $M \subset L(\mathbb{Q}_{\frac{m}{2^n}}), |M| = n, n \in \mathbb{N}$.

$$\forall V_k \in M, \exists R_i \in \mathbf{R}(\mathbb{Q}_{\frac{m}{2^n}}), R_i \in \mathbf{R}(\mathbb{Q}), i \in [0, l]:$$

$$V_k(x_1, ..., x_{l_k}) = R_0 + R_1 \cdot x_1 + R_2 \cdot x_2 + ... + R_{l_k} \cdot x_{l_k}.$$

Пусть $\deg(M) = d$. Обозначим максимальный по модулю числитель чисел из множества $U_0(M)$ через h_0, а максимальный по модулю числитель чисел из $U_1(M)$ через h_1. Пусть $h = \max(h_0, h_1)$. Максимальную арность автоматов из M обозначим через l.

Будем предполагать, что каждый автомат $V \in M$ задан при помощи $U(V)$, причем каждый многочлен $P(\xi), R(\xi)$ задаётся своими коэффициентами, каждый из которых задаётся парой чисел - числителем и знаменателем. В таком представлении требуется $O(n \cdot l \cdot d \cdot \log_2(h))$ бит памяти для представления системы M.

Теорема 2. *Задача проверки непринадлежности конечной системы* $M \subset L(\mathbb{Q}_{\frac{m}{2^n}})$ *предполным классам* $T_p, M_p, T_{int}, T_{\geq 0}, D, V_{\boldsymbol{P}}$, $\forall p, \forall \boldsymbol{P}$, *где* $p-$ *простые, отличные от двойки и* $\boldsymbol{P}$ *- непустые подмножества простых чисел, отличных от двойки, является алгоритмически разрешимой. Проверка непринадлежности* M *указанным классам потребует* $O(l^{n+1} \cdot n \cdot \log_2(h))$ *арифметических операций над целыми числами, где* l, n, h *определены как упомянуто выше.*

Доказательство. Заметим, что $\forall R = \frac{P(\xi)}{Q(\xi)} \in \mathbf{R}(\mathbb{Q}_{\frac{m}{2^n}})$, заданных отношением многочленов как упомняуто выше, за константное число арифметических операций определяются коэффициенты $R[0], R[1]$:

$$P(\xi) = a_0 + a_1 \cdot \xi + a_2 \cdot \xi^2 + ... + a_t \cdot \xi^t,$$
$$Q(\xi) = b_0 + b_1 \cdot \xi + b_2 \cdot \xi^2 + ... + b_r \cdot \xi^r,$$
$$R[0] = \frac{a_0}{b_0}, R[1] = \frac{a_1 - R[0] \cdot b_1}{b_0}.$$

Проверка непринадлежности T_{int} и $T_{\geq 0}$ сводится к сравнению с нулем или единицей не более $2 \cdot l \cdot n$ целых чисел (числителей или знаменателей коэффициентов в первый такт), что дает оценку по числу арифметических операций $O(l \cdot n)$.

Для проверки непринадлежности классам $T_p, M_p, \forall p$ - простых, отличных от двойки, будем применять алгоритм Евклида нахождения наибольшего общего делителя.
Оценка числа арифметических операций для алгоритма нахождения НОД двух чисел $a, b \in \mathbb{Z}$ алгоритмом Евклида составляет $O(\log_2(\min(a, b)))$[8]. Поскольку нам необходимо найти НОД не более $l \cdot n$ целых чисел (числителей коэффициентов во второй такт) для проверки непринадлежности классам M_p, и НОД не более n чисел (числителей свободных коэффициентов в первый такт) для проверки классов T_p, оценка числа арифметических операций, необходимых для отыскания двух наибольших общих делителей составляет $O(l \cdot n \cdot \log_2(h))$. Найденные наибольшие общие делители за $O(\log_2(h))$ арифметических операций освободим от кратности двойкам. Если любой из двух итоговых результатов отличен от 1, можем утверждать принадлежность некоторому M_p или T_p. Оценка числа арифметических операций составляет $O(l \cdot n \cdot \log_2(h))$.

По определению $V_{\mathbf{P}}$, если $\exists \mathbf{P}$ - конечное непустое подмножество простых чисел, отличных от двойки, такое что $M \in V_{\mathbf{P}}$, то $\forall V \in M$:

$$V(x_1, .., x_l) = R_0 + \textstyle\sum_{i=1}^{l} R_i \cdot x_i,$$
$$\forall i \in [0, l], R_i \in \mathbf{R}(\mathbb{Q}_{\frac{m}{2^n}}), |\{R_j | R_j[0] \neq 0, j \in [1, l]\}| = l',$$

с точностью до переименования входов выполнено хотя бы одно из следующих условий:

1) $l' \leq 1$.

2) $\exists i \in [1,k] : R_j[0] \vdots p_i, \forall j \in [1,l]$.

3) $R_j[0] \vdots p_1 \cdot p_2 \cdot ... \cdot p_k, \forall j \in [2,l]$.

Оценка числа арифметических операций для проверки первого условия у всех автоматов в M составляет $O(n \cdot l)$, поскольку потребуется сравнить с нулем не более $n \cdot l$ чисел. Автоматы множества M, для которых первое условие выполнено, могут далее не рассматриваться, поскольку они принадлежат всякому $V_{\mathbf{P}}$.

Для каждого $V_t \in M, V_t(x_1,..,x_q) = R_0^{(t)} + \sum_{i=1}^{l_t} R_i^{(t)} \cdot x_i$ найдем $c_t = \gcd(R_1^{(t)}[0], R_2^{(t)}[0], ..., R_{l_t}^{(t)}[0])$, что потребует $O(n \cdot l \cdot \log_2(h))$ арифметических операций. После этого вычислим $c = \gcd(c_1, c_2, ..., c_n)$, что потребует $O(n \cdot \log_2(h))$ арифметических операций. С использованием $O(\log_2(h))$ арифметических операций освободим число c от кратности двойкам. Отличие полученного результата от 1 будет говорить о принадлежности некоторому $V_{\mathbf{P}}$. Таким образом проверяется второе условие с использованием не более $O(n \cdot l \cdot \log_2(h))$ операций. Более того, все автоматы V_t для которых $\exists p > 2$ - простое, такое что c_t кратно p могут далее не рассматриваться, поскольку $V_t \in V_{\{p\}}$.

Для каждого $V_t \in M, V_t(x_1,..,x_q) = R_0^{(t)} + \sum_{i=1}^{l_t} R_i^{(t)} \cdot x_i$ зафиксируем номер i_t, такой что $1 \leq i_t \leq l_t$. Получим комбинацию чисел $(i_1, i_2, ..., i_n)$, всего таких комбинаций будет не более l^n. Каждой комбинации поставим в соответствие множество $M_j = \{R_i^{(k)}[0] | 1 \leq k \leq n, 1 \leq i \leq l_k, i \neq i_k\}$. Для вского M_j вычислим c_j - наибольший общий делитель элементов M_j, для фиксированного M_j это займет $O(l \cdot n \cdot \log_2(h))$ арифметических операций. Учитывая что число комбинаций не превышает l^n оценка числа арифметических операций составит $O(l^{(n+1)} \cdot n \cdot \log_2(h))$. Каждое c_j освободим от кратности двойкам и полученный результат сравним с единицей, это займет $O(l^n \cdot \log_2(h))$ операций. В случае неравенства любого из полученных чисел единице можем утверждать принадлежность некоторому $V_{\mathbf{P}}$, если же все числа оказываются равны единице – M не лежит ни в одном $V_{\mathbf{P}}$. Итоговая оценка числа арифметических операций составляет $O(l^{(n+1)} \cdot n \cdot \log_2(h))$.

Поскольку непринадлежность всем $V_{\mathbf{P}}$ влечет за собой непринадлежность D[7], теорема доказана. □

Автор выражает признательность своему научному руководителю, кандидату физ.-мат. наук, доценту кафедры МаТИС Часовских Анатолию Александровичу за помощь в постановке и решении задачи.

Список литературы

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

[2] Буевич В.А., "О полноте, A-полноте и t-полноте в классе автоматных отображений", *Интеллектуальные системы*, **10**:1-4 (2006), 613–638

[3] Бабин Д.Н., Летуновский А.А., "О возможностях суперпозиции, при наличии в базисе автоматов фиксированной добавки из булевых функций и задержки", *Интеллектуальные системы. Теория и приложения*, **19**:3 (2015), 15–22

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

[5] Chasovskikh A.A., "Completeness problem for the class of linear automata functions", *Discrete Mathematics and Applications*, **26**:2 (2016), 89–104

[6] Ронжин Д.В., "Линейные автоматы над полем рациональных чисел", *Интеллектуальные системы. Теория и приложения*, **21**:4 (2017), 144–155

[7] Ронжин Д.В., "Об условиях A-полноты линейных автоматов над двоично-рациональными числами", *Дискретная математика*, **32**:2 (2020), 45–62

[8] Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К., *Алгоритмы: построение и анализ, 3-е издание*, М.:«Вильямс», 2013, 1328 с.

References

[1] Kudryavcev V.B., Aleshin S.V., Podkolzin A.S., *Introduction to automata theory*, Nauka, Moscow, 1985, 320 c.

[2] Buyevich V.A., "About completeness, A-completeness and t-completness in the class of automata mappings.", *Intellectual systems.*, **10**:1-4 (2006), 613–638

[3] Babin D.N., Letunovskiy A.A., "About superposition potential, with having boolean functions and delay element as an addition to basis.", *Intellectual systems. Theory and applications.*, **19**:3 (2015), 15–22

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

[5] Chasovskikh A.A., "Completeness problem for the class of linear automata functions.", *Discrete Mathematics and Applications*, **26**:2 (2016), 89–104

[6] Ronzhin D.V., "Linear automata over the field of rational numbers.", *Intellectual systems. Theory and applications.*, **21**:4 (2017), 144–155

[7] Ronzhin D.V., "About A-completeness conditions for the automata over dyadic rationals.", *Discrete Mathematics*, **32**:2 (2020), 45–62

[8] Cormen, Thomas H.; Leiserson, Charles E.; Rivest, Ronald L.; Stein, Clifford., *Introduction to Algorithms. Third Edition.*, MIT Press, 2009, 1320 c.

A-completeness recognition for finite systems with additives of linear automata over the ring of dyadic rationals

Ronzhin D.V.

This work concerns questions of A-completeness of finite systems of linear automata over the ring of dyadic rationals. Condition of completeness of linear automata system, which includes automaton that models addition in the first step is described. For the formulated set of maximum subclasses in the class of linear automata over the ring of dyadic rationals decidability of a problem of finite set inclusion into these classes is proven.

Keywords: finite state automata, linear automata, dyadic rationals, A-completeness, maximum subclasses, decidability.