Задача определения порядка для автоматов, чьи функции переходов и выходов принадлежат замкнутому классу Поста

Н. В. Муравьев[1]

Рассматривается задача определения порядка автомата Мили относительно операции суперпозиции.

Доказано разбиение решетки Поста замкнутых классов относительно разрешимости задачи вычисления порядка для соответствующих R-автоматов.

Ключевые слова: автоматы Мили, классы Поста, алгоритмическая разрешимость.

1. Введение

Определение порядка элемента в полугруппе является классической задачей в алгебре. Несмотря на то, что в общем случае она алгоритмически неразрешима даже в группе конечных автоматных функций [1], автору ранее удалось найти богатые классы линейных автоматов, для которых не только существует алгоритм вычисления порядка относительно суперпозиции, но и есть точная верхняя оценка порядка автомата, зависящая от его размерности и базового поля [2, 3, 4, 5].

Таким образом, задачу можно решить, если на входном-выходном алфавите и множестве состояний удается ввести структуру линейного пространства. Естественно задаться вопросом: «какие еще структуры могут позволить алгоритмически определять порядок автоматной функции?». В настоящей работе мы вводим на алфавитах и множествах состояний структуру булевого куба. А функции переходов и выходов будут «уважать» эту структуру, если они принадлежат какому-нибудь фиксированному замкнутому классу Поста. Показано, что относительно алгоритмической разрешимости задачи для соответствующих классов автоматов решетку Поста можно разбить на две группы: классы, порождающие автоматы с неразрешимой задачей определения порядка, и классы, порождающие автоматы с разрешимой задачей определения порядка.

[1] *Муравьев Никита Валерьевич* — аспирант каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: ne-ki-tos@yandex.ru.

Muravev Nikita Valerievich — graduate student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

Полученные результаты уточняют границы разрешимости задачи определения порядка и дают нам новые нетривиальные классы автоматов, для которых она разрешима.

2. Технические леммы и основной результат

Рассматриваем инициальные автоматы Мили вида $G = (\Sigma, Q, \Sigma, \phi, \psi, q_0)$, чей входной-выходной алфавит является многомерным булевым кубом $\Sigma = E_2^n$, а множество состояний является произвольным подмножеством булевого куба $Q \subset E_2^m$.

Для замкнутого класса Поста $R \subset \mathbb{P}_2$ мы говорим, что автомат G является R-автоматом, если его функции переходов и выходов принадлежат этому классу $\phi, \psi \in R$. Нетрудно убедиться, что суперпозиция двух R-автоматов вновь будет R-автоматом.

Имеет место следующая

Теорема 1. *Задача определения порядка алгоритмически неразрешима в классе R-автоматов, если R содержит в себе один из следующих классов как подмножество: $F_2^\infty, F_6^\infty, D_2$. В противном случае задача определения порядка алгоритмически разрешима (рис. 1).*

Несмотря на то, что замкнутых классов бесконечное число, для доказательства этого результата нам понадобится рассмотреть лишь конечное число классов. Это следует из технических лемм, аналоги которых уже неоднократно встречались в литературе [6, 7]:

Лемма 1. *Рассмотрим замкнутые классы $R_1 \subset R_2 \subset \mathbb{P}_2$. Если не существует алгоритма определения порядка для R_1-автоматов, то его не существует и для R_2-автоматов.*

Доказательство. Лемма тривиально следует из того факта, что любой R_1-автомат является также и R_2-автоматом. А значит, если бы алгоритм существовал для R_2-автоматов, то он же подошел бы и для любого R_1-автомата. □

Лемма 2. *Рассмотрим замкнутые классы $R_1 \subset R_2 \subset \mathbb{P}_2$. Если существует алгоритм определения порядка для R_2-автоматов, то он же подходит для определения порядка R_1-автоматов.*

Доказательство. Очевидно, что любой R_1-автомат является также и R_2-автоматом. Следовательно, алгоритм для R_2-автоматов подойдет и для R_1-автоматов. □

Для замкнутого класса $R \subset \mathbb{P}_2$ мы обозначаем через R^* двойственный ему класс – класс, состоящий из двойственных функций. Для R-автомата G мы обозначаем через G^* двойственный ему автомат, у которого все функции переходов и выходов заменены на двойственные.

Лемма 3. *Рассмотрим замкнутый класс $R \subset \mathbb{P}_2$. Алгоритм определения порядка для R-автоматов существует тогда и только тогда, когда он существует для R^*-автоматов.*

Доказательство. Рассмотрим произвольный автомат $G \in R$. По свойствам двойственности

$$(G^n)^* = (G^*)^n,$$

$$G^n = G^k \Leftrightarrow (G^n)^* = (G^k)^* \Leftrightarrow (G^*)^n = (G^*)^k.$$

То есть, порядки автоматов G и G^* совпадают. Следовательно, для определения порядка одного из них достаточно определить порядок другого. И алгоритм, подходящий для R-автоматов, можно применить к R^*-автоматам, если рассматривать двойственные к ним автоматы того же порядка.

□

Заметим, что мы сознательно требуем в определении R-автомата того, чтобы входной-выходной алфавит Σ и множество состояний Q были целыми булевыми кубами, а не подмножествами булевых кубов. Это сужает класс рассматриваемых автоматов, что усиливает результаты об алгоритмической неразрешимости, но ослабляет результаты о разрешимости. Мотивацией для такого решения стала неудача в попытке обнаружить алгоритм определения порядка для S_6- и P_6-автоматов, у которых входной-выходной алфавит является собственным подмножеством булевого куба. Автор полагает, что такой алгоритм существует, и надеется, что в будущем результат удастся обобщить на более широкий класс автоматов.

3. Доказательство теоремы о классификации

Данный раздел посвящен доказательству основного результата работы, а именно теоремы 1 о классификации классов Поста по разрешимости задачи определения порядка для соответствующих автоматов.

Доказательство. Фактически мы хотим показать, что имеет место следующее разбиение решетки Поста (рис. 1). По леммам 1, 2 для этого достаточно доказать алгоритмическую неразрешимость задачи для F_2^∞-,F_6^∞-,D_2-автоматов и разрешимость для S_6-,L_1-,P_6-автоматов.

Для доказательства неразрешимости задачи мы покажем, что любой автомат может быть изоморфно вложен в F_2^∞-, F_6^∞-, D_2-автоматы, функционирующие схожим образом. Тогда неразрешимость будет следовать из неразрешимости в общем случае [1].

Неразрешимость для D_2-автоматов. Класс D_2 является пересечением монотонных и самодвойственных функций. Рассмотрим произвольный конечный автомат G. Закодируем его входной-выходной алфавит Σ наборами вида $0...010...0 \in \Sigma'$, где длина набора из Σ' не меньше трех. Закодируем множество состояний Q наборами вида $10...010...0 \in \{1\} \times Q'$, где длина набора из Q' не меньше трех, больше длины набора из Σ', и длина набора из $\Sigma' \times \{1\} \times Q'$ нечетная.

Доопределим функции выходов и переходов на остальных наборах так, чтобы они были монотонными и самодвойственными. Без ограничения общности рассмотрим функцию ϕ_1, определяющую значение первого элемента набора, кодирующего состояние. Для каждого набора вида $x1q,\ x \in \Sigma', q \in Q'$ эта функция задает значение $\phi_1(x1q) \in E_2$. Для самодвойственности мы должны доопределить ее на противоположных наборах следующим образом: $\phi_1(\bar{x}0\bar{q}) = \overline{\phi_1(x1q)}$. Для монотонности доопределяем функцию ϕ_1 на некоторых сравнимых с $x1q$ или $\bar{x}0\bar{q}$ наборах: если значение функции равно 0, то на всех меньших наборах тоже полагаем ее равной 0; если значение равно 1, то на всех больших наборах тоже полагаем ее равной 1. Процесс однозначен, так как все наборы $x1q, \bar{x}0\bar{q}$ попарно несравнимы. В самом деле, иначе существовали бы такие наборы $x, x' \in \Sigma',\ q, q' \in Q'$, что $x'1q' > \bar{x}0\bar{q}$, но наборы x, x', q, q' содержат по одной единице и $|x|, |q| > 2$ (по условию кодировки). А значит, наборы $\bar{x}, \bar{q}$ содержат как минимум по две единицы и неравенство $x'1q' > \bar{x}0\bar{q}$ невозможно. Осталось доопределить функцию ϕ_1 на всех остальных наборах. Положим ее равной 0 на всех оставшихся наборах, где число единиц меньше, чем нулей. Положим ее равной 1 на всех оставшихся наборах, где число единиц больше, чем нулей (здесь мы пользуемся нечетностью длины наборов, кодирующих пару из входной буквы и состояния). Очевидно, что такое определение сохраняет монотонность и самодвойственность. Аналогично доопределяем остальные функции ϕ_i, ψ_j.

Полученный D_2-автомат в точности изоморфен автомату G на множестве входных букв Σ'. На остальных буквах из $E^n \setminus \Sigma'$ автомат либо функционирует так же, как на сравнимых наборах из Σ', либо переходит в состояние из одних нулей или одних единиц и становится константным. Действительно, если значение функции ϕ_1 на наборе xlq, где $l \in E_2$, определялось количеством единиц в xlq, то и для всех остальных функций ϕ_i, ψ_j оно будет определяться так же: $\forall i, j, \phi_1(xlq) = \phi_i(xlq) = \psi_j(xlq)$. То есть, входная буква x переводит автомат в состояние из одних нулей или одних единиц, а на выходе мы тоже получаем набор из одних нулей или

одних единиц. Если мы рассматриваем суперпозицию исходного автомата с самим собой несколько раз, то этот набор из одних нулей или одних единиц будет распространяться по всем копиям исходного автомата и переводить их в такие же состояния. Так как длина кодировки состояния больше длины кодировки входной буквы, попавший в состояние из одних нулей или одних единиц автомат никогда из него не выйдет и будет константным. То есть, порядок полученного D_2-автомата совпадает с порядком исходного автомата G.

Неразрешимость для F_2^∞-, F_6^∞-автоматов. Класс F_6^∞ состоит из монотонных функций f, обладающих следующими свойствами: $f(a,...,a) = a$ и все наборы x, на которых $f(x) = 1$, имеют общую единицу. Рассмотрим произвольный конечный автомат G. Закодируем его входной-выходной алфавит Σ наборами вида $0...010...0 \in \Sigma'$. Закодируем множество состояний Q наборами вида $10...010...0 \in \{1\} \times Q'$.

Теперь нам нужно доопределить функции переходов и выходов на остальных наборах. Без ограничения общности рассмотрим функцию ϕ_1, определяющую значение первого элемента набора. Для монотонности, доопределяем функцию ϕ_1 на некоторых сравнимых с $x1q, x \in \Sigma', q \in Q'$ наборах: если значение функции равно 0, то на всех меньших наборах тоже полагаем ее равной 0; если значение равно 1, то на всех больших наборах тоже полагаем ее равной 1. На всех оставшихся наборах полагаем ϕ_1 равной нулю. Очевидно, полученная функция ϕ_1 монотонна, обладает α-свойством ($\phi_1(a,...,a) = a$) и все наборы, на которых она обращается в единицу, имеют общую единицу (в начале кодировки состояния). Аналогично доопределяем остальные функции ϕ_i, ψ_j.

Полученный F_6^∞-автомат изоморфен автомату G на множестве входных букв Σ'. На остальных буквах из $E^n \setminus \Sigma'$ автомат либо функционирует так же, как на сравнимых наборах из Σ', либо переходит в состояние из одних нулей и становится константным, выдавая наборы из нулей. То есть, порядок полученного F_6^∞-автомата совпадает с порядком исходного автомата G. Для F_2^∞-автоматов утверждение следует из леммы 3.

Теперь докажем разрешимость задачи для нижней части решетки.

Разрешимость для L_1-автоматов. Разрешимость для L_1-автоматов следует из разрешимости для линейных автоматов над произвольным конечным полем [2, 4].

Разрешимость для S_6-,P_6-автоматов. Рассмотрим класс S_6-автоматов. Их канонические уравнения содержат только константы и дизъюнкции, а значит, их можно представить в виде

$$\begin{cases} q(t+1) = Aq(t) \vee Bx(t), \\ y(t) = Cq(t) \vee Dx(t), \\ q(0) = q_0, \end{cases}$$

где A, B, C, D - матрицы над E_2, а матричное умножение использует обычное умножение и дизъюнкцию вместо обычного сложения. При таком подходе мы рассматриваем булев куб E_2 как полукольцо (кольцо без вычитания), множество состояний и алфавит как полумодули (как модули, но над полукольцом вместо кольца), а матрицы A, B, C, D как гомоморфизмы этих полумодулей. Кроме того, сложение в E_2 (и в любых многочленах и рядах над ним) идемпотентно ($a \vee a = a$), то есть E_2 – коммутативный диоид. Этот факт позволяет нам воспользоваться следующей теоремой [8]:

Теорема 2. *Пусть S есть произвольный коммутативный диоид и $A \in S^{p\times p}$. Тогда существуют такие $c \geq 1, N \in \mathbb{N}$, что для любых $1 \leq i, j \leq p$ и любого $l \in \{0, ..., c-1\}$ найдется конечное семейство скаляров $\alpha_1, \lambda_1, ..., \alpha_k, \lambda_k$, такое, что*

$$\forall n \geq N,\ A_{ij}^{nc+l} = \bigoplus_{r=1}^{k} \alpha_r \lambda_r^{n-N}.$$

Аналогично случаю линейных автоматов, мы можем описать действие S_6-автомата G с помощью передаточной функции $M(z) = \bigvee_{v=0}^{\infty} CA^vBz^{v+1} \vee D$ и сдвига $S(z) = \bigvee_{v=0}^{\infty} CA^v q_0 z^v$.

$$y(z) = M(z)x(z) \vee S(z).$$

$M(z)$ – это матрица над коммутативным диоидом, а потому к ней применима теорема 2 и

$$\forall t \geq N,\ M_{ij}^{tc+l}(z) = \bigvee_{r=1}^{k} \alpha_r(z)\lambda_r^{t-N}(z).$$

Заметим, что, для произвольного $l \in \{0, ..., c-1\}$ верно

$$\#\{M_{ij}^{tc+l}\}_{t\geq N} < \infty \ \Leftrightarrow\ \#\{M_{ij}^{t}\}_{t\geq 0} < \infty,$$

а значит, для определения порядка передаточной функции нам достаточно рассмотреть одно произвольное значение l. Для фиксированных i, j, l возможны следующие случаи:

1) $\alpha_r(z) = 0$ или $\lambda_r(z) = 0$. Очевидно, $\mathrm{ord}(\alpha_r(z)\lambda_r^{t-N}(z)) < \infty$.

2) $\langle \lambda_r(z), z^0 \rangle = 0$. Тогда минимальная степень z в $\alpha_r(z)\lambda_r^{t-N}(z)$ будет расти с ростом t и $\mathrm{ord}(\alpha_r(z)\lambda_r^{t-N}(z)) = \infty$.

3) $\langle \lambda_r(z), z^0 \rangle = 1$ и $\lambda_r(z) \notin E_2[z]$. Получается, $\lambda_r(z)$ бесконечный ряд с единицей. При его возведении в степень возможно лишь добавление новых слагаемых. Так как он периодический, добавление нового слагаемого происходит с добавлением бесконечного числа других слагаемых со

сдвигом равным длине периода ряда. Так как период конечен, то конечно и число возможных рядов при возведении $\lambda_r(z)$ в степень. А значит, $\mathrm{ord}(\alpha_r(z)\lambda_r^{t-N}(z)) < \infty$.

4) $\langle \lambda_r(z), z^0 \rangle = 1$, $\lambda_r(z) \in E_2[z]$ и $\alpha_r(z) \in E_2[z]$. В таком случае $\lambda_r(z)$ и $\alpha_r(z)$ многочлены, и, очевидно, что $\mathrm{ord}(\alpha_r(z)\lambda_r^{t-N}(z)) = \infty$.

5) $\langle \lambda_r(z), z^0 \rangle = 1$, $\lambda_r(z) \in E_2[z]$ и $\alpha_r(z) \notin E_2[z]$. Аналогично случаю (3), с ростом n возможно лишь добавление новых слагаемых, причем добавляются они сразу со всеми сдвигами, кратными длине периода. Следовательно, $\mathrm{ord}(\alpha_r(z)\lambda_r^{t-N}(z)) < \infty$.

Ясно, что мы можем определить порядок и конечной суммы таких рядов $M_{ij}^{tc+l}(z) = \bigvee_{r=1}^{k} \alpha_r(z)\lambda_r^{t-N}(z)$. Таким образом, мы умеем определять порядок каждого элемента матрицы $M(z)$. Если порядки всех элементов передаточной функции конечны, то есть конечен порядок самой передаточной функции, то очевидно, конечен и порядок всего автомата. Также порядок конечен, если начиная с какого-то момента все коэффициенты в сдвиге $S(z)$ равны единицам.

Пусть существует элемент $S_i(z)$ в векторе $S(z)$ с нулевым коэффициентом при бесконечном числе мономов z^k. Рассмотрим соответствующую строку $M_i(z)$ матрицы $M(z)$. Если в ней все элементы имеют конечный порядок, то, очевидно, порядок автомата по этой координате тоже конечен. Если же имеется хотя бы один элемент M_{ij} бесконечного порядка, то при возведении матрицы в степень у него будет расти либо максимальная, либо минимальная степень. Рассмотрим входной вектор $x(z)$, такой что $x_j(z) = z^q$ для произвольного q, а для всех остальных координат l он равен нулю $x_l(z) = 0$. Если периоды в $S_i(z)$ и $M_{ij}^N(z)$ не совпадают, то порядок автомата на входе $x(z)$ бесконечный. Если периоды совпадают, то нужно выбрать число q в $x_j(z) = z^q$ так, чтобы минимальная или максимальная степень в $M_{ij}^t(z)x_j(z)$ всегда соответствовала нулевому сдвигу в $S_i(z)$. В таком случае порядок автомата на входе $x(z)$ тоже будет бесконечным. А значит, будет бесконечным и порядок самого автомата. Повторяем процедуру для всех координат. Получили алгоритм проверки конечности порядка автомата. Для P_6-автоматов утверждение следует из леммы 3. Теорема доказана.

□

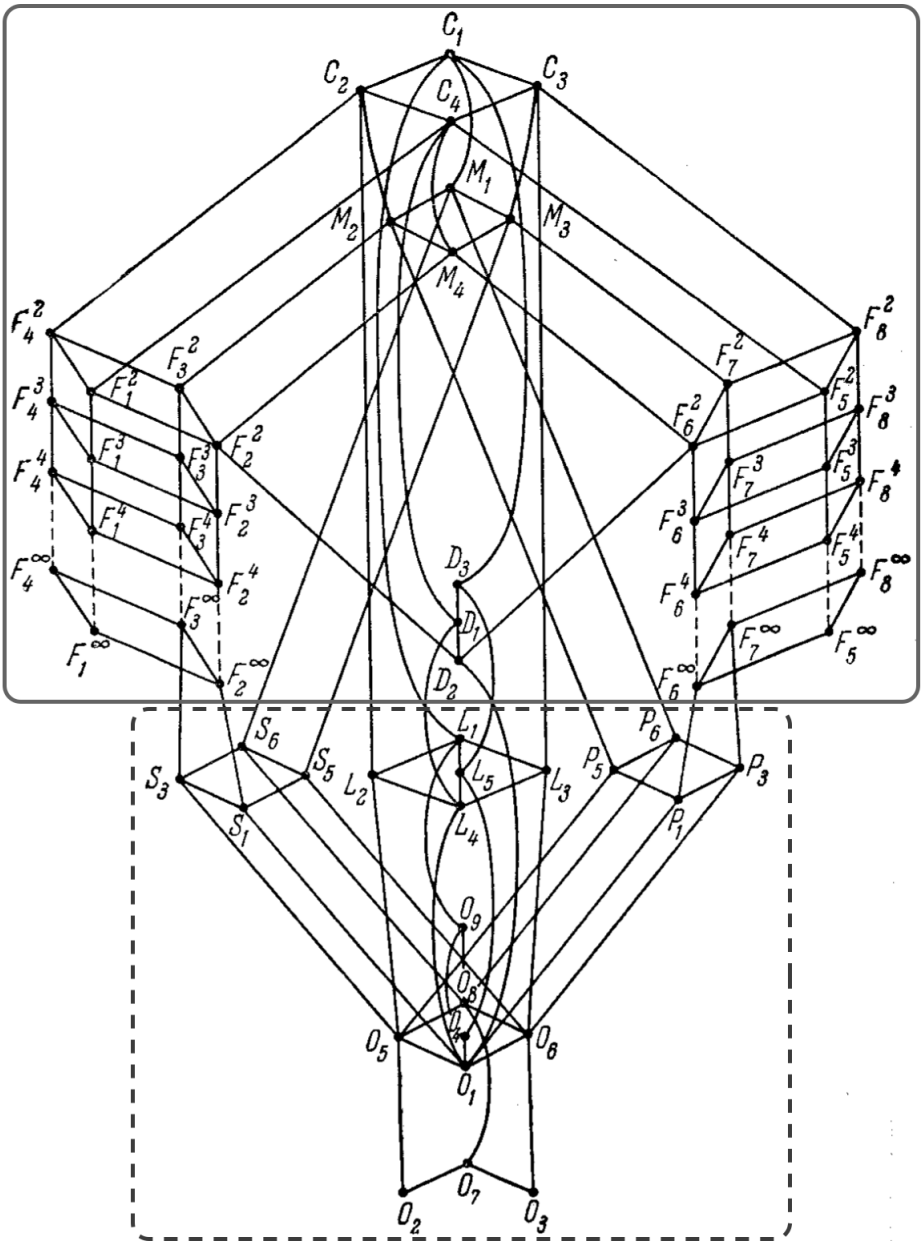

Рис. 1. Решетка Поста замкнутых классов $\mathbb{P}_2$ (схема взята из [9]). Сплошным прямоугольником выделены классы, для которых алгоритмически неразрешима задача определения порядка в соответствующем классе автоматов. Пунктирным прямоугольником выделены классы, порождающие классы автоматов с разрешимой задачей определения порядка.

Список литературы

[1] P. Gillibert, “An automaton group with undecidable order and Engel problems”, *Journal of Algebra*, **497** (2018), 363–392.

[2] Муравьев Н.В., “Разрешимость задачи определения порядка линейного автомата”, *Интеллектуальные системы. Теория и приложения*, **24**:2 (2020), 145–155.

[3] Муравьев Н.В., “О порядках линейных над полем рациональных чисел автоматов”, *Интеллектуальные системы. Теория и приложения*, **24**:4 (2020), 119–124.

[4] Муравьев Н.В., “Оценки порядков линейных автоматов”, *Вестник Московского университета. Серия 1: Математика, Механика*, 2022, № 6, 8–14.

[5] Муравьев Н.В., “Максимальные конечные порядки линейных автоматов над произвольным полем”, *Вестник Московского университета. Серия 1: Математика, Механика*, 2024, № 5, 71–73.

[6] Бабин Д.Н., “О классификации автоматных базисов Поста по разрешимости свойств полноты и A-полноты”, *Доклады академии наук*, **367**:4 (1999), 439–441.

[7] Бабин Д.Н., “Разрешимость задачи полноты автоматного базиса в зависимости от его булевой части”, *Вестник Московского университета. Серия 1: Математика, Механика*, 2019, № 1, 52–54.

[8] Stéphane Gaubert, “On rational series in one variable over certain dioids. [Research Report] RR-2162, inria-00074510 INRIA”, 1994.

[9] Яблонский С.В., Гаврилов Г.П., Кудрявцев В.Б., *Функции алгебры логики и классы Поста*, "Наука", 1966.

The order problem for automata which transition and output functions lie in closed Post classes

Muravev N.V.

We consider the order problem for Mealy automata with respect to the superposition operation.

The splitting of the Post's lattice of closed classes is proved based on decidability of the order problem for respective R-automata.

Keywords: Mealy automata, Post classes, algorithmic decidability.

References

[1] P. Gillibert, “An automaton group with undecidable order and Engel problems”, *Journal of Algebra*, **497** (2018), 363–392.

[2] N.V. Muravev, “Decidability of the order problem for linear automata”, *Intelligent systems. Theory and applications*, **24**:2 (2020), 145–155.

[3] N.V. Muravev, “About orders of linear over rationals automata”, *Intelligent systems. Theory and applications*, **24**:4 (2020), 119–124.

[4] N.V. Muravev, “Bounds on Orders of Linear Automata”, *Moscow University Mathematics Bulletin*, 2022, №6, 8–14.

[5] N.V. Muravev, “Maximal Finite Orders of Linear Automata over an Arbitrary Field”, *Moscow University Mathematics Bulletin*, 2024, №5, 71–73.

[6] D.N. Babin, “On classification of automata Post basises based on decidability of completeness and A-completeness”, *Reports of the Academy of Science*, **367**:4 (1999), 439–441.

[7] D.N. Babin, “Solvability of the Problem of Completeness of Automaton Basis Depending on its Boolean Part”, *Moscow University Mathematics Bulletin*, 2019, №1, 52–54.

[8] Stéphane Gaubert, “On rational series in one variable over certain dioids. [Research Report] RR-2162, inria-00074510 INRIA”, 1994.

[9] Yablonsky S.V., Gavrilov G.P., Kudryavtsev V.B., *Functions of the logic algebra and Post classes*, "Nauka", 1966.