О порядках линейных над полем рациональных чисел автоматов

Муравьев Н.В.[1]

Рассматривается задача определения порядка инициального линейного над полем рациональных чисел автомата относительно операции суперпозиции. Выведена верхняя оценка на порядок автомата, зависящая от размерности.

Ключевые слова: линейные автоматы, порядок в полугруппе.

1. Введение

Если входной и выходной алфавиты инициального автомата совпадают, то число различных автоматов, получаемых суперпозицией исходного с самим собой, может быть как конечным, так и бесконечным. Задача определения порядка конечного инициального автомата относительно суперпозиции алгоритмически неразрешима в общем случае [1]. Но для некоторых классов автоматов удается найти алгоритмы определения порядка. Например, Алешин С.В. показал [3], что в группе одномерных (вход и выход - элементы поля) линейных автоматов над полем из двух элементов автомат имеет конечный порядок тогда и только тогда, когда его переходы безусловны. Этот результат обобщается на одномерные автоматы над любым полем.

Ранее автором была доказана верхняя граница на порядок линейного автомата над конечным полем [7], что позволило получить алгоритм решения задачи для автоматов произвольной размерности над конечными полями. В данной работе этот результат будет распространен на случай поля рациональных чисел. А именно, будет выведена верхняя оценка на порядок линейного над $\mathbb{Q}$ автомата, зависящая от его размерности.

Работа существенно использует известные результаты в теории линейных автоматов [2, 3, 4, 5, 6], в частности метод передаточных функций.

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

Muravev Nikita Valerevich — student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, The Department of Mathematical Theory of Intellectual Systems.

2. Основные определения и утверждения

Определение 2.1. Линейным автоматом над полем рациональных чисел $\mathbb{Q}$ называется инициальный абстрактный автомат $(\Sigma, Q, \Omega, \phi, \psi, q_0)$, чьи множество состояний Q, входной Σ и выходной Ω алфавиты есть подмножества конечномерных векторных пространств над $\mathbb{Q}$, а канонические уравнения имеют следующий вид:

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

где $q(t) \in Q, x(t) \in \Sigma, y(t) \in \Omega$; A, B, D, L - линейные операторы между соответствующими пространствами.

Без ограничения общности везде далее считаем, что размерности линейных оболочек алфавитов и линейных оболочек множеств состояний совпадают с размерностями соответствующих векторных пространств, подмножествами которых они являются.

Определение 2.2. Размерностью линейного автомата будем называть размерность линейной оболочки его входного-выходного алфавита.

Будем обозначать поле частных кольца многочленов над $\mathbb{Q}$ от переменной z как $Frac(\mathbb{Q}[z])$.

Следующая лемма есть обобщение известных результатов [2, 6, 7]. Мы приводим ее без доказательства.

Лемма 1. *Сопоставим каждому слову $x = x_0x_1x_2x_3... \in \Sigma^\infty$ формальный ряд*

$$x(z) = \sum_{v=0}^{\infty} x_v z^v,$$

А каждому слову $y = y_0y_1y_2y_3... \in \Omega^\infty$ - формальный ряд

$$y(z) = \sum_{v=0}^{\infty} y_v z^v.$$

Тогда для любого n-мерного линейного автомата G существуют передаточная функция $M_G(z) \in (Frac(\mathbb{Q}[z]))^{n\times n}$ и сдвиг $S_G(z) \in (Frac(\mathbb{Q}[z]))^n$, такие что для любых $x \in \Sigma^\infty, y \in \Omega^\infty$

$$y = G(x) \Leftrightarrow y(z) = M_G(z)x(z) + S_G(z).$$

Определение 2.3. Порядком автомата будем называть порядок его автоматной функции относительно суперпозиции.

3. Основные результаты

Введем следующие обозначения:

$\phi(m)$ - функция Эйлера, считающая количество натуральных чисел меньших m, которые взаимнопросты с m;

НОК - наименьшее общее кратное;

$\psi(n) := \max\{m \in \mathbb{N} : \phi(m) \leq n\}$.

Теорема 1. *Если порядок n-мерного линейного над $\mathbb{Q}$ автомата конечен, то он не превосходит*

$$\max_{1 \leq v_1 < \ldots < v_n \leq \psi(n)} HOK(v_1, \ldots, v_n).$$

Доказательство. Пусть порядок n-мерного линейного над $\mathbb{Q}$ автомата G конечен. Тогда конечен порядок его передаточной функции $M_G(z)$. По лемме 1 передаточная функция $M_G(z)$ есть линейный оператор над полем $Frac(\mathbb{Q}[z])$, а значит она есть линейный оператор и над полем $Frac(\mathbb{C}[z])$. Порядок оператора конечен, а значит конечны и порядки по умножению его собственных значений (ведь при возведении матрицы в степень собственные значения тоже возводятся в степень). Следовательно собственные значения, лежащие в алгебраическом замыкании поля $Frac(\mathbb{C}[z])$, имеют конечные порядки. Но тогда они либо нули, либо корни из единицы. Все корни из единицы в алгебраическом замыкании поля $Frac(\mathbb{C}[z])$ лежат в $\mathbb{C}$, так как $\mathbb{C} \subset Frac(\mathbb{C}[z])$ алгебраически замкнуто, и при его расширении новых корней добавиться не может. То есть коэффициенты характеристического многочлена с одной стороны лежат в $\mathbb{C}$ (так как получаются сложением и умножением собственных значений), а с другой стороны лежат в $Frac(\mathbb{Q}[z])$ (так как получаются сложением и умножением элементов матрицы передаточной функции). Значит коэффициенты принадлежат $\mathbb{C} \cap Frac(\mathbb{Q}[z]) = \mathbb{Q}$.

Получили, что коэффициенты характеристического многочлена передаточной функции есть константы из $\mathbb{Q}$, а корни этого многочлена есть комплексные корни из единицы и, возможно, ноль. Но минимальный многочлен над $\mathbb{Q}$ для корня из единицы k-й степени это круговой многочлен

$$\prod_{\substack{1 \leq m \leq k \\ \text{НОД}(m,k)=1}} (\lambda - e^{2i\pi m/k})$$

порядка $\phi(k)$, где НОД означает наибольший общий делитель. То есть, если собственное значение передаточной функции n-мерного автомата G есть корень из единицы степени k, то $\phi(k) \leq n$. А значит

$$k \leq \psi(n) := \max\{m \in \mathbb{N} : \phi(m) \leq n\}.$$

Таким образом, получена верхняя оценка на порядок собственных значений передаточной функции автомата. Теперь рассмотрим Жорданову нормальную форму передаточной функции. Это блочно-диагональная матрица с клетками вида

$$\begin{pmatrix} \lambda & 1 & 0 & 0 & ... \\ 0 & \lambda & 1 & 0 & ... \\ ... & ... & ... & ... & ... \\ ... & ... & 0 & \lambda & 1 \\ ... & ... & 0 & 0 & \lambda \end{pmatrix}$$

на диагонали.

Если $\lambda = 0$, порядок клетки равен ее размерности. Если λ есть корень k-й степени из единицы, порядок клетки конечен тогда и только тогда, когда ее размерность равна единице, и равен k. Порядок передаточной функции есть наименьшее общее кратное порядков клеток.

Из вышесказанного следует, что порядок передаточной функции не превосходит

$$\max_{1 \le v_1 < ... < v_n \le \psi(n)} \text{НОК}(v_1, ..., v_n).$$

Однако автомат определяется не только своей передаточной функцией, но и сдвигом. Сдвиг автомата G^n имеет вид

$$(M_G^{n-1}(z) + ... + M_G(z) + I)S_G(z).$$

Если k, l наименьшие натуральные числа, для которых $M_G^k(z) = M_G^l(z)$, $k < l$, то либо $(M_G^{l-1}(z) + ... + M_G^k(z))S_G(z) = 0$ и порядок автомата совпадает с числом различных степеней его передаточной функции, либо $(M_G^{l-1}(z) + ... + M_G^k(z))S_G(z) \neq 0$ и порядок автомата бесконечен (так как $\mathbb{Q}$ есть поле характеристики 0).

То есть, если порядок n-мерного линейного над $\mathbb{Q}$ автомата конечен, то он не превосходит

$$\max_{1 \le v_1 < ... < v_n \le \psi(n)} \text{НОК}(v_1, ..., v_n).$$

□

Полученную оценку можно огрубить, чтобы получить более лаконичное неравенство. Известно [8], что $\forall n > 6\ \phi(n) \ge \sqrt{n}$. Значит $\forall n > 6\ \psi(n) \le n^2$. Тогда $\forall n > 6$

$$\max_{1 \le v_1 < ... < v_n \le \psi(n)} \text{НОК}(v_1, ..., v_n) \le \max_{1 \le v_1 < ... < v_n \le n^2} \text{НОК}(v_1, ..., v_n) \le$$

$$\le n^2 \cdot ... \cdot (n^2 - (n-1)) = \frac{(n^2)!}{(n^2 - n)!}.$$

То есть порядок n-мерного линейного над $\mathbb{Q}$ автомата либо бесконечен, либо не превышает $\frac{(n^2)!}{(n^2-n)!}$ при $n > 6$.

Для $n \leq 6$ верхнюю границу на порядок можно вычислить по теореме. Обозначив за $L(n)$ максимальный порядок n-мерных линейных над $\mathbb{Q}$ автоматов, получаем следующее следствие из теоремы 1:

Следствие 1.1.

$$L(1) \leq 2$$

$$L(2) \leq 30$$

$$L(3) \leq 60$$

$$L(4) \leq 4\,620$$

$$L(5) \leq 13\,860$$

$$L(6) \leq 2\,450\,448$$

$$L(n) \leq \frac{(n^2)!}{(n^2-n)!},\ n > 6.$$

Заметим, что обобщение полученных результатов на случай автоматов над полями вещественных и комплексных чисел невозможно. Уже среди двумерных автоматов с одним состоянием над полем вещественных чисел имеются автоматы сколь угодно больших порядков.

В самом деле, возьмем примитивный корень n-й степени из единицы $a + ib$ в поле комплексных чисел. Рассмотрим двумерный линейный над $\mathbb{R}$ автомат с одним состоянием:

$$\begin{pmatrix} y_1(t) \\ y_2(t) \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix}.$$

Очевидно, порядок этого автомата равен порядку матрицы

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

по умножению.

Ее Жорданова нормальная форма имеет вид

$$\begin{pmatrix} a+ib & 0 \\ 0 & a-ib \end{pmatrix}.$$

То есть порядок матрицы равен n.

Таким образом показано, что для линейных автоматов над $\mathbb{R}$ не существует верхней границы на порядок, зависящей от размерности.

Автор выражает благодарность своему научному руководителю Бабину Д.Н. за помощь на всех этапах подготовки и написания данной работы.

Список литературы

[1] P. Gillibert, “An automaton group with undecidable order and Engel problems”, *preprint, available online at arxiv.org/abs/1710.09733*, 2017.

[2] Кудрявцев В.Б., Алешин С.В., Подколзин А.С., *Введение в теорию автоматов*, "Наука", Москва, 1985.

[3] Алешин С.В., *Алгебраические системы автоматов.*, "МАКС Пресс", Москва, 2016.

[4] Бабин Д.Н., “Автоматы с линейными переходами”, *Интеллектуальные системы. Теория и приложения*, **23**:3 (2019), 87-95.

[5] Часовских А.А., “О полноте в классе линейных автоматов”, *Математические вопросы кибернетики*, 1995, № 3, 140–166.

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

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

[8] Kendall D.G., Osborn H.B., “Two Simple Lower Bounds for Euler’s Function”, *Texas Journal of Science*, **17** (1965).

About orders of linear over rationals automata

Muravev N.V.

We consider the order problem with respect to the superposition operation for linear automata over rational numbers. An upper bound of automata orders is proved.

Keywords: linear automata, order in semigroup.