Разрешимость задачи определения порядка линейного автомата

Муравьев Н.В.[1]

Рассматривается задача определения порядка линейного автомата. Доказан критерий конечности порядка линейного автомата, позволяющий решать задачу алгоритмически. Дана верхняя оценка на порядок линейного автомата.

Ключевые слова: конечные автоматы, линейные автоматы, порядок в полугруппе.

1. Введение

В 2017 году Pierre Gillibert доказал [1], что задача определения порядка элемента в автоматной группе (группе, порожденной конечным автоматом) алгоритмически неразрешима. Позже этот результат был усилен Bartholdi и Митрофановым [2]. В частности из него следует, что, начиная с некоторого n, задача определения порядка элемента неразрешима и в группе всех обратимых автоматов AS_n. Представляет интерес нахождение таких классов автоматов, для которых задача разрешима.

Одним из важнейших классов конечных автоматов с выходом является класс линейных автоматов. Данное семейство автоматов имеет большое значение как с теоретической, так и с практической точек зрения. На сегодняшний день существует большое количество книг [3] и статей [7, 8], посвященных этой тематике.

Ранее Алешин С.В. показал [5], что в группе одномерных линейных автоматов над полем из двух элементов автомат имеет конечный порядок тогда и только тогда, когда его переходы безусловны. В данной работе

[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.

этот результат будет обобщен на линейные автоматы любой размерности над произвольным конечным полем. Более того, будет выведена верхняя оценка на порядок линейного автомата, зависящая от его размерности и поля, над которым он линеен.

2. Базовые определения и утверждения

Определение 2.1. Абстрактным инициальным конечным автоматом (далее автомат) называется шестерка $(\Sigma, Q, \Omega, \phi, \psi, q_0)$, где

Σ - конечное непустое множество, называемое входным алфавитом,
Q - конечное непустое множество, называемое множеством состояний,
Ω - конечное непустое множество, называемое выходным алфавитом,
$\phi : \Sigma \times Q \to Q$ - функция переходов,
$\psi : \Sigma \times Q \to \Omega$ - функция выходов,
$q_0 \in Q$ - начальное состояние.

Определение 2.2. Заметим, что всякий автомат U с начальным состоянием q_0 задает отображение $f_{U_{q_0}} : \Sigma^* \to \Omega^*$, определенное индуктивно и называющееся автоматной функцией:

1) $f_{U_{q_0}}(\varepsilon) = \varepsilon$, где ε - пустое слово
2) $a \in \Sigma \Rightarrow f_{U_{q_0}}(a) = \psi(a, q_0)$
3) $a_0 a \in \Sigma^*, a_0 \in \Sigma \Rightarrow f_{U_{q_0}}(a_0 a) = \psi(a_0, q_0) f_{U_{\phi(a_0, q_0)}}(a)$.

Определение 2.3. Автоматы, задающие одинаковые автоматные функции, называются эквивалентными.

Определение 2.4. Два состояния автоматов (двух разных или одного и того же) называются эквивалентными, если инициальные автоматы с началом в этих состояниях эквивалентны.

Определение 2.5. Автоматы, между множествами состояний которых существует биекция, переводящая состояния в эквивалентные им, называются изоморфными.

Известна следующая теорема [4]:

Теорема 1. *Для каждого автомата существует единственный с точностью до изоморфизма эквивалентный автомат с наименьшим возможным количеством состояний.*

Такой автомат называется минимальным или приведенным для исходного автомата.

В дальнейшем мы зачастую будем отождествлять понятия инициального автомата U_{q_0} и его автоматной функции $f_{U_{q_0}}$, если это не будет вызывать путаницы.

При совпадении входного и выходного алфавитов множество обратимых автоматных функций (обратимых автоматов) образует группу относительно суперпозиции, которую мы будем обозначать AS_n, где n - мощность входного-выходного алфавита.

Если отказаться от требования обратимости, то мы получим полугруппу с единицей (моноид) автоматных функций. Этот моноид обозначим AP_n, где n - мощность входного-выходного алфавита.

Очевидно, что при разных алфавитах одной и той же мощности соответствующие группы (моноиды) автоматов изоморфны, так что данное обозначение корректно.

Определение 2.6. Каноническими уравнениями автомата $U = (\Sigma, Q, \Omega, \phi, \psi, q_0)$ называется следующая система уравнений:

$$\begin{cases} q(t+1) = \phi(q(t), x(t)) \\ y(t) = \psi(q(t), x(t)) \\ q(0) = q_0, \end{cases}$$

где $t \in \mathbb{N} \cup \{0\}, q(t) \in Q, x(t) \in \Sigma, y(t) \in \Omega$.

Ясно, что эта система задает функцию $f_{U_{q_0}}$, а именно

$$f_{U_{q_0}}(x(0)x(1)x(2)...) = y(0)y(1)y(2)... \quad \forall x(t) \in \Sigma, t \in \mathbb{N} \cup \{0\}.$$

Определение 2.7. Абстрактный инициальный автомат $(\Sigma, Q, \Omega, \phi, \psi, q_0)$ назовем линейным над конечным полем F_m (где m - мощность поля), если его множество состояний Q, входной Σ и выходной Ω алфавиты есть подмножества конечномерных векторных пространств над F_m, 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.

Ввиду изоморфизма конечномерных линейных пространств одинаковой размерности над общим полем, в дальнейшем будем всегда полагать, что линейные пространства имеют вид F_m^n, где n - размерность.

Лемма 1. *После минимизации линейного над F_m автомата мы получаем автомат, изоморфный некому линейному над тем же полем.*

Доказательство. Пусть мы склеили два эквивалентных состояния линейного автомата. Если два состояния эквивалентны, то они реализуют одну и ту же функцию, а значит их разность реализует ту же функцию, что и нулевой вектор (нулевое состояние). Получается, что если состояния q_1 и q_2 эквивалентны, то и состояния $q, q + k(q_1 - q_2)$ эквивалентны для любых $q \in Q, k \in F_m$. А значит мы можем спроецировать пространство состояний на любую гиперплоскость (подпространство коразмерности один), не параллельную $q_1 - q_2$, (это линейное отображение) и домножить слева линейные операторы в функции переходов на оператор проецирования, получив автомат, эквивалентный исходному. Повторяем данную процедуру, пока не придем к приведенному автомату. Получили линейный минимальный автомат, эквивалентный исходному. □

Данная лемма показывает, что при изучении линейных автоматов мы можем ограничиться лишь минимальными (приведенными) автоматами.

Далее все автоматы считаются приведенными.

Заметим, что обратимость линейного автомата эквивалентна обратимости оператора L из его канонических уравнений на линейной оболочке $\langle\Sigma\rangle$.

Лемма 2. *Суперпозиция линейных над F_m автоматов есть линейный над F_m автомат.*

Доказательство. Пусть имеется линейный автомат G с каноническими уравнениями

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

и линейный автомат G' над тем же полем, чей выходной алфавит совпадает с входным алфавитом автомата G и заданный каноническими уравнениями

$$\begin{cases} q'(t+1) = A'q'(t) + B'x(t) \\ y(t) = D'q'(t) + L'x(t) \\ q'(0) = q'_0. \end{cases}$$

Тогда ясно, что их суперпозиция $G \circ G'$ задается следующими каноническими уравнениями:

$$\begin{cases} \begin{pmatrix} q'(t+1) \\ q(t+1) \end{pmatrix} = \begin{pmatrix} A' & 0 \\ BD' & A \end{pmatrix} \begin{pmatrix} q'(t) \\ q(t) \end{pmatrix} + \begin{pmatrix} B' \\ BL' \end{pmatrix} x(t) \\ y(t) = \begin{pmatrix} LD' & D \end{pmatrix} \begin{pmatrix} q'(t) \\ q(t) \end{pmatrix} + LL'x(t) \\ \begin{pmatrix} q'(0) \\ q(0) \end{pmatrix} = \begin{pmatrix} q'_0 \\ q_0 \end{pmatrix}. \end{cases}$$

То есть суперпозиция есть линейный автомат. □

Теорема 2. *Обратный автомат к линейному эквивалентен линейному над тем же полем.*

Доказательство. Пусть имеется линейный обратимый автомат G с каноническими уравнениями

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

Докажем, что обратным к нему будет автомат G' с со следующими каноническими уравнениями:

$$\begin{cases} q'(t+1) = (A - BL^{-1}D)q'(t) + BL^{-1}x(t) \\ y(t) = -L^{-1}Dq'(t) + L^{-1}x(t) \\ q'(0) = q_0, \end{cases}$$

где L^{-1} - обратный оператор к сужению L на $\langle\Sigma\rangle$, произвольно продолженный на все пространство.

Рассмотрим их суперпозицию $G \circ G'$:

$$\begin{cases} \begin{pmatrix} q'(t+1) \\ q(t+1) \end{pmatrix} = \begin{pmatrix} A - BL^{-1}D & 0 \\ -BL^{-1}D & A \end{pmatrix} \begin{pmatrix} q'(t) \\ q(t) \end{pmatrix} + \begin{pmatrix} BL^{-1} \\ BL^{-1} \end{pmatrix} x(t) \\ y(t) = \begin{pmatrix} -D & D \end{pmatrix} \begin{pmatrix} q'(t) \\ q(t) \end{pmatrix} + LL^{-1}x(t) \\ \begin{pmatrix} q'(0) \\ q(0) \end{pmatrix} = \begin{pmatrix} q_0 \\ q_0 \end{pmatrix}. \end{cases} \Rightarrow$$

$$\overset{q(t)=q'(t)}{\Rightarrow} \begin{cases} \begin{pmatrix} q'(t+1) \\ q(t+1) \end{pmatrix} = \begin{pmatrix} (A - BL^{-1}D)q(t) \\ (A - BL^{-1}D)q(t) \end{pmatrix} + \begin{pmatrix} BL^{-1} \\ BL^{-1} \end{pmatrix} x(t) \\ y(t) = x(t) \\ \begin{pmatrix} q'(0) \\ q(0) \end{pmatrix} = \begin{pmatrix} q_0 \\ q_0 \end{pmatrix}. \end{cases}$$

То есть G' - обратный к G. □

Следствие 2.1. *Множество линейных над F_m автоматов с совпадающими входными-выходными алфавитами Σ образует моноид относительно суперпозиции.*

Обозначим этот моноид LP_Σ.

Следствие 2.2. *Множество обратимых линейных над F_m автоматов с совпадающими входными-выходными алфавитами Σ образует группу относительно суперпозиции.*

Обозначим эту группу LS_Σ.

3. Определение порядка автомата в моноиде LP_Σ

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 3.1. Порядком элемента в полугруппе будем называть мощность подполугруппы, порожденной данным элементом.

Определение 3.2. С каждым линейным автоматом G

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

свяжем два формальных ряда:

$$M_G(z) = \sum_{v=0}^{\infty} DA^v Bz^{v+1} + L,$$

$$S_G(z) = \sum_{v=0}^{\infty} DA^v q_0 z^v.$$

Назовем их передаточной функцией и сдвигом соответственно.

Для произвольного поля K обозначим $Frac(K[z])$ поле частных кольца многочленов над K от переменной z.

Следующие две леммы являются обобщениями известных результатов [4]. Для сокращения изложения мы опустим их доказательства.

Лемма 3. *Для любого линейного автомата G над полем F_m его передаточная функция $M_G(z)$ есть линейный оператор над полем $Frac(F_m[z])$*

Лемма 4. *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 линейного автомата G и любых $x \in \Sigma^\infty, y \in \Omega^\infty$

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

Лемма 4 позволяет нам переформулировать задачи для линейных автоматов в терминах передаточных функций и сдвигов. Например верна

Лемма 5. *Пусть G есть линейный над F_m автомат, тогда его порядок конечен тогда и только тогда, когда $\exists k, n \in \mathbb{N} : M_G^k(z) = M_G^n(z), k \neq n$.*

Доказательство. По определению порядок автомата конечен, когда конечна порожденная им полугруппа. То есть в бесконечной последовательности $G, G^2, G^3, ...$ есть лишь конечное число различных элементов, а значит $\exists k, n \in \mathbb{N} : G^k = G^n, k \neq n$. Из леммы 4 и замечания о том, что линейные оболочки алфавитов совпадают с содержащими их векторными пространствами, следует, что по автомату однозначно определяется его передаточная функция, а значит

$$G^k = G^n \Rightarrow M_G^k(z) = M_G^n(z).$$

Теперь докажем, что из существования таких различных $k, n \in \mathbb{N}$, что $M_G^k(z) = M_G^n(z)$, следует конечность порядка автомата G. Если $M_G^k(z) = M_G^n(z)$, то $M_G^{k+l}(z) = M_G^{n+l}(z)$ для любого $l \in \mathbb{N}$. Получается, что последовательность передаточных функций степеней автомата периодическая с периодом $|n-k|$, а последовательность сдвигов степеней автомата имеет вид

$$S_G(z),\ (M_G(z)+I)S_G(z),\ (M_G^2(z)+M_G(z)+I)S_G(z),\ ...$$

где I - единичная матрица.

Из чего следует, что она тоже периодическая с периодом $p \cdot |n-k|$, где p - характеристика поля F_m. Но если последовательности передаточных функций и сдвигов периодические, то по лемме 4 и последовательность степеней автомата периодическая. □

Введем некоторые понятия, которые нам понадобятся в дальнейшем, и напомним несколько алгебраических свойств конечных полей.

Определение 3.3. Размерностью линейного автомата будем называть размерность линейной оболочки его входного-выходного алфавита.

Для любого простого p и любых натуральных m, n, таких что $m|n$, в поле F_{p^n} содержится ровно одно подполе порядка p^m.

Из этого следует, что имеет место следующая цепочка включений

$$F_p \subseteq F_{p^{2!}} \subseteq F_{p^{3!}} \subseteq ... \subseteq F_{p^{n!}} \subseteq ...$$

Известно, что корни многочлена порядка n над полем F_m лежат в поле F_{m^n}.

Из этого следует, что $F_{p^\infty} = \bigcup_{k=1}^{\infty} F_{p^{k!}}$ является алгебраическим замыканием поля F_{p^n} при любом натуральном n и простом p.

Теперь мы готовы доказать основную теорему.

Теорема 3. *Порядок линейного над F_m автомата конечен тогда и только тогда, когда коэффициенты характеристического многочлена его передаточной функции есть константы из поля F_m.*

Доказательство. По лемме 5 порядок линейного над F_m автомата G конечен тогда и только тогда, когда конечен порядок его передаточной функции $M_G(z)$.

Пусть порядок n-мерного автомата G конечен. Тогда конечен порядок его передаточной функции. По лемме 3 передаточная функция есть линейный оператор над полем $Frac(F_m[z])$, а значит она линейный оператор и над полем $Frac(F_{p^\infty}[z])$. 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 $Frac(F_{p^\infty}[z])$, имеют конечные порядки. Но тогда они либо нули, либо корни из единицы. А все корни из единицы в поле $Frac(F_{p^\infty}[z])$ лежат в F_{p^∞}. Это позволяет переписать уравнение на собственные значения

$$\sum_{i=0}^{n}(a_{i,k}z^k + ...a_{i,1}z + a_{i,0})\lambda^i = 0,\ a_{i,j} \in F_m, k \in \mathbb{N} \cup \{0\}$$

в виде системы

$$\begin{cases} a_{n,k}\lambda^n + ... + a_{1,k}\lambda + a_{0,k} = 0 \\ ... \\ a_{n,0}\lambda^n + ... + a_{1,0}\lambda + a_{0,0} = 0. \end{cases}$$

Получили систему линейных уравнений над полем F_m. Как было замечено ранее, ее решения лежат в поле F_{m^n}. Следовательно собственные значения передаточной функции лежат в поле F_{m^n}. Но тогда и коэффициенты характеристического многочлена лежат в F_{m^n}. С другой стороны коэффициенты характеристического многочлена есть произведения и суммы элементов матрицы $M_G(z)$, то есть они принадлежат полю $Frac(F_m[z])$. Итого коэффициенты характеристического многочлена для передаточной функции $M_G(z)$ лежат в $Frac(F_m[z]) \cap F_{m^n} = F_m$. Что и требовалось показать.

Осталось доказать теорему в другую сторону. Если коэффициенты характеристического многочлена передаточной функции автомата есть константы из поля F_m, то порядок автомата конечен.

Обозначим эти коэффициенты $M_0, ..., M_{n-1}$ и запишем характеристический многочлен:

$$\lambda^n + M_{n-1}\lambda^{n-1} + ... + M_0.$$

По теореме Гамильтона-Кэли характеристический многочлен аннулирует свою матрицу, то есть

$$M_G(z)^n + M_{n-1} \cdot M_G(z)^{n-1} + ... + M_0 = 0.$$

Данное равенство можно домножить на $M_G(z)^{s-n}$ для любого $s > n$ и получить

$$M_G(z)^s + M_{n-1} \cdot M_G(z)^{s-1} + ... + M_0 \cdot M_G(z)^{s-n} = 0.$$

Таким образом мы выразили s-ю степень (при $s > n$) передаточной функции автомата через линейную комбинацию с константными коэффициентами предыдущих n степеней. Следовательно всякая степень передаточной функции есть линейная комбинация с константными коэффициентами первых n степеней передаточной функции (начиная с нулевой). Таких комбинаций конечное число, ведь их коэффициенты принадлежат конечному полю F_m. А значит и порядок передаточной функции конечен. Откуда следует конечность порядка всего автомата. □

Следствие 3.1. *Порядок n-мерного линейного над F_m автомата G не превышает $p(m^n - 1)$, где p - характеристика поля F_m.*

Доказательство. При доказательстве предыдущей теоремы было показано, что степень передаточной функции $M_G(z)$ есть линейная комбинация с константными коэффициентами первых n степеней передаточной функции. Так как коэффициенты принадлежат полю F_m, всего таких комбинаций m^n. Однако заметим, что комбинация из одних нулей возможна тогда и только тогда, когда передаточная функция нильпотентна, и в таком случае ее порядок не превышает n. Если же она не нильпотентна, мы имеем лишь $m^n - 1$ возможных комбинаций. Итого порядок передаточной функции не превышает $max\{m^n - 1, n\} = m^n - 1$.

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 $M_G^k(z) = M_G^l(z), \quad k < l,$ 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 равен $l - 1 + (p - 1)(l - k)$. Заметим, что $l - 1$ есть порядок передаточной функции $M_G(z)$ и $l - k \leq l - 1$. То есть порядок автомата не превышает $p(m^n - 1)$. □

В заключение автор выражает благодарность своему научному руководителю Бабину Д.Н. за постановку задачи и ценные указания и замечания по ходу 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] L. Bartholdi, I. Mitrofanov, "The word and order problems for self-similar and automata groups", *preprint, available online at arxiv.org/abs/1710.10109*, 2017.

[3] Гилл А., *Линейные последовательностные машины*, "Наука", Москва, 1974.

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

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

[6] Винберг Э.Б., *Курс алгебры (2-е изд.)*, "Факториал Пресс", Москва, 2001.

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

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

Decidability of the order problem for linear automata
Muravev N.V.

We consider the order problem for linear automata. A finite order criterion for linear automata is presented that provides an algorithm solving this problem. An upper bound of linear automata orders is proved.

Keywords: finite automata, linear automata, order in semigroup.