

Алгебраические конструкции в теории автоматов

С. В. Алёшин

Теория автоматов оперирует с широким кругом алгебраических объектов и средств. В годы становления этой теории алгебраические методы активно использовались для решения ее внутренней проблематики. Со временем оказалось, что уже методы теории автоматов могут с успехом применяться в алгебраических исследованиях.

Первой систематической работой, в которой раскрывались связи алгебры и теории автоматов, была статья В. М. Глушкова [1]. В последующих работах набор алгебраических объектов, связанных с автоматами, расширился, в нем были как классические группы, полугруппы, кольца, пространства, так и алгебраические системы, ранее не возникавшие в математических исследованиях.

Особое место в теории автоматов заняли алгебраические конструкции, связанные с (конечными) полугруппами. С конечным автоматом $\mathcal{A} = (A, Q, B, \varphi, \psi)$, где A, B , соответственно, входной и выходной алфавиты, Q — множество состояний, $\varphi : A \times Q \rightarrow Q$ — функция переходов, $\psi : A \times Q \rightarrow B$ — функция выходов, можно связать полугруппу подстановок на множестве Q . Каждая буква $a \in A$ входного алфавита действует на Q как подстановка $\varphi_a : Q \rightarrow Q$, $\varphi_a(q) = \varphi(q, a)$. Последовательное действие букв a_1 и a_2 соответствует произведению подстановок φ_{a_1} и φ_{a_2} :

$$\varphi_{a_1 a_2} : Q \rightarrow Q, \quad \varphi_{a_1 a_2}(q) = \varphi_{a_2}(\varphi_{a_1}(q)).$$

Таким образом множество $\langle \varphi_a \mid a \in A \rangle$ порождает конечную полугруппу $P_{\mathcal{A}}$, называемую внутренней полугруппой автомата \mathcal{A} . Очевидно, что $P_{\mathcal{A}}$ является гомоморфным образом свободной полугруппы A^* (A^* — множество всех слов в алфавите A).

Методы теории конечных полугрупп были применены для решения важной задачи декомпозиции автоматов, то есть представления автомата в виде соединения более «простых» автоматов. Оказалось, что эти методы хорошо работают в случае, когда автомат можно разложить в суперпозицию автоматов. Среди многих работ 1960-х годов, посвященных этому направлению, центральное место занимает работа Крона и Роудза [2], которым удалось показать, как внутренняя полугруппа автомата суперпозиции связана с внутренними полугруппами автоматов — компонентов соединения.

Оказалось, что если выход автомата $\mathcal{A}_1 = (A_1, Q_1, B, \varphi_1, \psi_1)$ соединить с входом автомата $\mathcal{A}_2 = (B, Q_2, C, \varphi_2, \psi_2)$, то полугруппа полученного автомата-суперпозиции является подполугруппой сплетения полугруппы автомата \mathcal{A}_1 и полугруппы автомата \mathcal{A}_2 . Напомним, что сплетение полугруппы P_1 подстановок на множестве Q_1 и полугруппы P_2 подстановок на множестве Q_2 — это полугруппа P подстановок на декартовом произведении $Q_1 \times Q_2$. Элементами P являются пары (p, f) , $p \in P_1$, $f \in F$, где F — множество функций из Q_1 в P_2 ,

$$F = \{f \mid f : Q_1 \rightarrow P_2\},$$

а действие пары (p, f) на $Q_1 \times Q_2$ определяется следующим образом

$$(p, f)[q_1 q_2] = [q'_1, q'_2], \quad q'_1 = p[q_1], \quad q'_2 = f(q_1)[q_2].$$

Здесь $w[x]$ обозначает действие подстановки w на элемент x .

Можно видеть, что операция сплетения имеет «автоматный» вид. В самом деле, рассмотрим устройство, на вход которого поступают пары $[q_1, q_2]$.

В «начальном состоянии» устройство перерабатывает первый элемент q_1 пары (q_1, q_2) в элемент $p[q_1]$, при этом устройство переходит в состояние, зависящее от q_1 , и в этом состоянии перерабатывает второй элемент q_2 пары (q_1, q_2) в элемент $f(q_1)[q_2]$. Таким образом, устройство определяет действие подстановки (p, f) сплетения полугрупп P_1 и P_2 .

Итак, с каждым автоматом можно связать его (внутреннюю) полугруппу. С другой стороны, абстрактной полугруппе P соответствует (бесконечно) много автоматов, внутренняя полугруппа каждого из

которых — это полугруппа подстановок, изоморфная P . В частности, можно рассмотреть автомат $S_p = (P, P, P, *, *)$, у которого входной и выходной алфавиты и множество состояний совпадают с множеством элементов P , функции переходов и выходов определяются «таблицей умножения» в P .

$\varphi(p, p') = p * p'$, $\psi(p, p') = p * p'$, где $*$ — операция умножения в P .

Такой автомат назовем специальным автоматом полугруппы P . В упомянутой работе [2] дана полная характеристика разложений автомата на компоненты, которые являются специальными автоматами.

Центральной задачей теории автоматов является задача о выразимости. Если указан набор Σ операций, с помощью которых из данных автоматов можно строить новые, то этот набор определяет оператор замыкания I на множестве автоматов. Для заданного множества автоматов M множество $I(M)$ — это все автоматы, которые получаются многократным применением операций из Σ к автоматам M . Для двух множеств M_1 и M_2 решение задачи выразимости с оператором замыкания I состоит в проверке включения $I(M_1) \subseteq I(M_2)$.

В работе [2] была решена эта задача для случая, когда M_2 состоит из специальных автоматов полугрупп и, кроме того, содержит все автоматы без памяти (операторы). В качестве операций рассматривались операции суперпозиции. При всей важности работы [2] в ней присутствовало сильное ограничительное требование рассматривать в качестве компонентов разложения специальные автоматы. Ниже мы вернемся к этому вопросу.

Бесконечные полугруппы и группы стали объектами изучения в теории автоматов с конца 1960-х годов. Зафиксируем конечный алфавит $A = (a_1 \dots a_m)$ и рассмотрим множество P_A всех автоматных отображений множества A^* всех слов в алфавите A в себя. Каждое такое отображение реализуется некоторым конечным инициальным автоматом $\mathcal{A} = (A, Q, A, \varphi, \psi, q_0)$. На множестве P_A естественно определяется операция суперпозиции отображений — если функция $F_1(x)$ вычисляется автоматом $\mathcal{A}_1 = (A, Q_1, A, \varphi_1, \psi_1, q_0^1)$ и $F_2(x)$ — автоматом $\mathcal{A}_2 = (A, Q_2, A, \varphi_2, \psi_2, q_0^2)$, то, соединяя выход \mathcal{A}_1 с входом \mathcal{A}_2 , мы построим автомат $\mathcal{A} = (A, Q, A, \varphi, \psi, q_0)$, у которого $Q = Q_1 \times Q_2$, и для $(q_1, q_2) \in Q_1 \times Q_2$

$$\begin{aligned}\varphi((q_1, q_2), a) &= (q'_1, q'_2), \\ q'_1 &= \varphi_1(q_1, a), \quad q'_2 = \varphi_2(q_2, \psi_1(q_1, a)), \\ \psi((q_1, q_2), a) &= \psi_2(q_2, \psi_1(q_1, a)), \quad q_0 = (q_0^1, q_0^2).\end{aligned}$$

Автомат \mathcal{A} реализует, очевидно, суперпозицию F функций F_1 и F_2 : $F(x) = F_2(F_1(x))$.

Введенная операция превращает P_A в полугруппу с единицей, роль которой играет автомат — «проводник», то есть автомат с одним состоянием, в котором реализуется тождественная подстановка на множестве A .

Нетривиальное свойство полугруппы P_A заключается в том, что в ней каждая порождающая система элементов приводима, то есть содержит собственную порождающую подсистему [3].

Если отображение $F_a : A^* \rightarrow A^*$, реализуемое конечным автоматом, является взаимно-однозначным, то обратное отображение также реализуется некоторым конечным автоматом (число состояний которого равно числу состояний \mathcal{A}). Таким образом, множество таких отображений составляет групповую часть полугруппы P_A . Эта группа получила название группы автоматных подстановок AS_n , $n = |A|$.

Группа AS_n^k оказалась исключительно интересным объектом, изучение которого уже позволило решить ряд трудных задач алгебры. Это финитно-аппроксимируемая группа — достаточно рассмотреть последовательность гомоморфных образов AS_n — группы $AS_n^{(k)}$, $k = 1, 2, \dots$. Группа AS_n^k состоит из ограничений на словах длины k отображений из AS_n , и является сплетением k экземпляров симметрической группы S_n [4].

$$AS_n^k = \underbrace{S_n \int S_n \int \dots \int S_n}_{k \text{ раз}}$$

Поскольку элементы AS_n реализуются конечными автоматами, каждый из этих элементов несет в себе след периодичности, индуцируемой соответствующим автоматом.

Так возникает гомоморфизм AS_n на группу, элементами которой являются периодические (с предпериодом) последовательности из 0

и 1, с операцией поразрядного сложения по $\text{mod } 2$ [5]. Кстати, доказательство существования неприводимой системы образующих (базиса) в группе AS_n из этой статьи содержит пробел, и вопрос о существовании базиса в AS_n остается открытым.

Интерес к изучению AS_n резко возрос после того, как С. В. Алёшин обнаружил связь этой группы с известной проблемой Бернсайда [6].

Проблема Бернсайда для периодических групп — всякая ли периодическая группа локально конечна — как оказалось, может быть решена средствами теории автоматов. В работе [6] для каждого простого числа p была построена бесконечная периодическая подгруппа Bp группы AS_p с двумя образующими, которая, очевидно, является и финитно-аппроксимируемой.

Группа B_2 — это 2-группа, каждый элемент которой имеет порядок, равный некоторой степени 2. Порядки элементов B_2 не ограничены в совокупности.

Конструктивность и финитность описания элементов AS_n с помощью автоматов дают возможность строить и изучать ее подгруппы с разными свойствами. В частности, с каждым (неинициальным) автоматом $\mathcal{A} = (A, Q, A, \varphi, \psi)$ можно связать набор инициальных автоматов $I = \{\mathcal{A}_i = (A, Q, A, \varphi, \psi, q_i), q_i \in Q\}$. Подгруппу AS_n , порожденную системой I , естественно назвать группой, порожденной автоматом \mathcal{A} , или коротко \mathcal{A} -группой. Обратной любой конечный набор инициальных автоматов $I = \{\mathcal{A}_i = (A, Q_i, A, \varphi_i, \psi_i, q_i)\}$, реализующих элементы AS_n , можно объединить в один автомат, взяв прямую сумму автоматов $\mathcal{A} = \sum_i \mathcal{A}_i = (A, Q, A, \varphi, \psi)$, у которой $Q = \bigcup_i Q_i$, и если $q \in Q_i$, то $\varphi(q, a) = \varphi_i(q, a)$, $\psi(q, a) = \psi_i(q, a)$.

Таким образом, любая конечно-порожденная подгруппа AS_n называется подгруппой некоторой \mathcal{A} -группы.

Уже группы, порождаемые автоматами с двумя и тремя состояниями, обладают рядом интересных свойств [7].

Так, например, среди групп, порождаемых автоматами с двумя состояниями, имеется группа Клейна, бесконечная циклическая группа, группа диэдра бесконечного порядка.

Примеры групп, построенных на основе конструкции из [6], дали ответ на некоторые важные вопросы алгебры [8]. Так, Р. И. Григор-

чук построил конечно порожденную подгруппу AS_n промежуточного роста, что решало проблему Милнора [9].

А. В. Рожков рассмотрел отображения, реализуемые обобщенными автоматами. Рассмотрим «автомат», на вход которого в момент t подаются буквы алфавита A_t , $\varphi = 1, 2, \dots$, его функции переходов и выходов также суть последовательности $\varphi = \{\varphi_t, t = 1, 2, \dots\}$, $\psi = \{\psi_t, t = 1, 2, \dots\}$, $\varphi_t : Q \times A_t \rightarrow Q$, $\psi_t : Q \times A_t \rightarrow A_t$.

Взаимно-однозначные отображения, реализуемые такими «автоматами», образуют (для фиксированной последовательности $\{A_t, t = 1, \dots\}$) группу, которую можно также рассматривать как группу автоморфизмов (бесконечного) дерева.

Подход А. В. Рожкова дал возможность изучения бесконечных групп, получивших название AT_w , построенных на основе конструкции С. В. Алёшина [10].

Если все алфавиты A_t , $t = 1, 2, \dots$ конечны и совпадают, мы получаем группу AS_n , для некоторого n .

Интерес представляют порождающие системы AS_n . В [11] показано, что AS_n порождается своими элементами бесконечного порядка. Можно показать, что каждый автомат из AS_n представим произведением автоматов, у которых лишь в одном состоянии реализуется нетривиальная подстановка на множестве букв входного алфавита. Однако неизвестно, какими могут быть порядки таких элементов AS_n кроме 2, 4 и бесконечность [11]. Открытым является и вопрос об алгоритмической разрешимости проблемы порядка элемента в AS_n — можно ли по заданной диаграмме автомата определить порядок элемента AS_n , который реализуется этим автоматом.

Конечные группы также изучаются с помощью теоретико-автоматных построений. Напомним, что внутренняя группа суперпозиции двух (групповых) автоматов \mathcal{A}_1 и \mathcal{A}_2 есть подгруппа сплетения внутренней группы автомата \mathcal{A}_1 и внутренней группы автомата \mathcal{A}_2 . При этом она является расширением группы первого автомата \mathcal{A}_1 . Какое именно расширение получается, зависит, в частности, от функции выходов «верхнего» автомата \mathcal{A}_1 , выход которого соединяется с входом автомата \mathcal{A}_2 . Варьируя выходные функции, можно «управлять» построением расширения, что дает сильное средство исследования получающихся групп.

Один из «вариантов» проблемы Бернсайда — так называемая ослабленная проблема Бернсайда — ставит вопрос о существовании максимальной конечной группы $B_0(d, m)$ с d образующими многообразия $x^m = 1$, при этом, как известно, вопрос сводится к изучению групп $B_0(d, p^n)$ для простых p .

В.И. Малыгин рассмотрел [12] расширения групп автоматов, получаемые присоединением «стандартного» автомата с внутренней группой Z_p . Пусть $G_{\mathcal{A}}$ — внутренняя группа автомата $\mathcal{A} = (A, Q, B, \varphi_1 \psi_1)$ с n состояниями, при этом $G_{\mathcal{A}}$ — группа из многообразия, определенного тождеством $V(z_1, \dots, z_r) = 1$. К выходу \mathcal{A} присоединяется вход автомата с абелевой внутренней группой. Для произвольного набора входных слов a_1, \dots, a_r слово $V(a_1, \dots, a_r) = 1$ в группе $G_{\mathcal{A}}$. Если выходное слово $\psi_1(q, V(a_1, \dots, a_r)) = 1$ в группе Z_p для любого состояния q автомата \mathcal{A} и любого набора a_1, \dots, a_r , то внутренняя группа суперпозиции \mathcal{A} и Z_p также принадлежит многообразию $V(z_1, \dots, z_r) = 1$. В аддитивной записи имеем $\psi_1(q, V(a_1, \dots, a_r)) = 0$. Если представить действие слова $\psi_1(q, V(\mathcal{A}_1, \dots, \mathcal{A}_r))$ как сумму действий букв $\psi_1(q, a)$, $q \in Q$, $a \in A$, то выражение $\psi_1(q, V(a_1, \dots, a_r)) = 0$ можно рассматривать как бесконечную (по всем a_1, \dots, a_r) систему линейных уравнений от неизвестных $\psi_1(q, a)$, $q \in Q$, $a \in A$.

В.И. Малыгину удалось преобразовать бесконечную систему в конечную, при этом возникло линейное пространство L векторов $(\psi_1(q, a)$, $q \in Q$, $a \in A$), таких, что расширение группы $G_{\mathcal{A}}$ снова принадлежит многообразию $V(z_1, \dots, z_r) = 1$. Изучая линейное пространство L для многообразия $z^{p^m} = 1$ (присоединяемый автомат с циклической группой Z_p), он получил оценки для порядка группы $B_0(d, p^m)$:

$$\begin{aligned} \text{если } b(d, p^m) &= \log_p |B_0(d, p^m)|, \\ \text{то } b(d, p^m) &\geq (d-1)p^{b(d, p^{m-1})} + b(d, p^{m-1}) + 1. \end{aligned}$$

Пространство Малыгина может стать инструментом и для изучения других многообразий.

Классический подход к построению групп состоит в оперировании с простыми группами, из которых, как из «неделимых атомов»

собираются группы с разными свойствами. Автоматные конструкции расширили набор «атомов», поскольку при построении автомата с внутренней группой G в качестве компонентов могут использоваться и автоматы с внутренними полугруппами. При этом существенно используется операция обратной связи, когда выход автомата соединяется с одним из входных каналов.

Так, например, из циклической группы Z_n может быть получена симметрическая группа S_n только с помощью операции обратной связи [13].

При рассмотрении так называемых линейных автоматов возникает алгебраическая система с тремя бинарными операциями — система $PR(\xi)$, $PR(\xi) = \{\mu(\xi) = \frac{U(\xi)}{V(\xi)} \mid U(\xi), SV(\xi) \in E_2[\xi], V(\xi) \notin \xi \cdot E_2[\xi]\}$, где $E_2[\xi]$ — кольцо многочленов над полем $E_2 = \{0, 1\}$, операции сложения и умножения — из поля частных $R(\xi) = \{\mu(\xi) = \frac{U(\xi)}{V(\xi)}, U(\xi), V(\xi) \in E_2[\xi]\}$, а третья операция $Q(\mu_1, \mu_2)$ — частичная, она применима к паре (μ_1, μ_2) , если $\mu_2 = \frac{U_2(\xi)}{V_2(\xi)}$, где $U_2(\xi) \in \xi E_2(\xi)$, при этом $Q(\mu_1, \mu_2) = \frac{\mu_1}{1+\mu_2}$.

Линейные автоматы над полем E_2 — это автоматы, которые строятся из сумматора $S(x_1x_2) = x_1 + x_2 \pmod{2}$ и задержки с начальным состоянием 1. Известно [14], что проблема полноты конечных систем автоматных функций в классе всех автоматных функций алгоритмически неразрешима. Для класса функций, вычисляемых линейными автоматами, проблема полноты конечных систем линейных автоматов оказалась алгоритмически разрешимой [15]. А. А. Часовских разработал для алгебраической системы $PR(\xi)$ технику, сходную с техникой расширений полей, заметив, что произвольной функции $f(x_1, \dots, x_n)$ можно сопоставить набор $\mu_1(\xi), \dots, \mu_n(\xi), \mu_o(\xi)$ из $PR(\xi)$, так что операции суперпозиции и обратной связи, примененные к функциям, сводятся к операциям над соответствующими наборами, при этом элементы получаемых наборов строятся из элементов исходных наборов с помощью трех указанных операций в $PR(\xi)$.

Таким образом, для решения «внутренних» задач теории автоматов с успехом используются алгебраические построения.

Упомянутая выше теорема Крона-Роудза алгебраическими средствами решила проблему выразимости автоматов в базисе, содержа-

щем специальные автоматы простых групп. Автоматные функции, реализуемые такими автоматами, имеют тем большее число переменных, чем выше порядок группы. Этот недостаток теоремы удается устранить [16], показав, что специальный автомат простой группы P можно заменить произвольным автоматом с внутренней группой, у которой P является гомоморфным образом подгруппы. В результате, например, известный результат Д. Н. Бабина [17] о полноте относительно суперпозиции множества автоматных функций двух переменных получил новое доказательство, которое опиралось на два факта из алгебры — 1) для любого n симметрическая группа S_n имеет 2 образующих (и потому реализуется автоматом с 1 бинарным входом), 2) если автоматная функция реализуется автоматом с внутренней группой, то имеется входное слово, равное единице в этой группе, которое попарно отличает все состояния автомата.

Итак, теория автоматов активно использует классические объекты из алгебры, а также вводит в рассмотрение новые алгебраические системы и предоставляет новые, «неклассические» конструкции.

Список литературы

- [1] Глушков В. М. Абстрактная теория автоматов // УМН. 1961. Т. XVI. Вып. 5.
- [2] Алгебраическая теория автоматов, языков и полугрупп / Под ред. М. Арбиба. М., 1975.
- [3] Алёшин С. В. Об отсутствии базисов в некоторых классах инициальных автоматов // Проблемы кибернетики. М., 1970. Вып. 22.
- [4] Заровный В. П. Автоматные подстановки и сплетения групп // ДАН СССР. 160. 1965. № 3.
- [5] Алёшин С. В. О базисах в группах автоматных подстановок // Дискретный анализ. Новосибирск, 1970. Вып. 17.
- [6] Алёшин С. В. Конечные автоматы и проблема Бернсайда о периодических группах // Математические заметки. 1972. Вып. 3.
- [7] Zuk A. Groupes engendrés par les automates // Seminaire Bourbaki. Vol. 2006–2007.

- [8] Каргаполов М. И., Мерзляков Ю. И. Основы теории групп // М., 1982.
- [9] Григорчук Р. И. К проблеме Милнора о групповом росте // ДАН СССР. 1983. 271. № 1.
- [10] Рожков А. В. К теории групп алешинского типа // Математические заметки. 1986. Т. 40. № 5.
- [11] Макаров В. В. О группах автоматных перестановок // Фундаментальная и прикладная математика. М.: МГУ, 1996. 2. № 1.
- [12] Малыгин В. И. Алгебраические инварианты композиций автоматов / Канд. дисс. 1988.
- [13] Малыгин В. И. Трансформации группы автомата под действием операции обратной связи // VI Всесоюзная конференция по теоретическим проблемам кибернетики. 1983.
- [14] Кудрявцев В. Б., Алёшин С. В., Подколзин А. С. Введение в теорию автоматов. М., 1985.
- [15] Часовских А. А. Об алгоритмической разрешимости проблемы полноты для линейных автоматов // Вестник МГУ. 1985. Сер. мат. Вып. 2.
- [16] Алёшин С. В. Об одном следствии теоремы Крона-Роудза // Дискретная математика. 1999. Т. 11. Вып. 4.
- [17] Бабин Д. Н. О полноте двуместных о.-д. функций относительно суперпозиции // Дискретная математика. 1989. 1. № 4.