

Б. М. ШАИН

СИММЕТРИЧНЫЕ КОНЕЧНЫЕ ПОЛУГРУППЫ ПРЕОБРАЗОВАНИЙ И ЯДЕРНЫЕ АВТОМАТЫ

(Представлено академиком В. М. Глушковым 12 XI 1971)

Полугруппа Φ преобразований множества A (под преобразованиями понимаются полные, т. е. всюду определенные преобразования) называется транзитивной, если для любых $a_1, a_2 \in A$ найдется $\varphi \in \Phi$, для которого $\varphi(a_1) = a_2$; Φ называется симметричной, если для любых $a_1, a_2 \in A$ и $\varphi \in \Phi$ из того, что $\varphi(a_1) = a_2$, следует существование $\psi \in \Phi$, для которого $\psi(a_2) = a_1$.

В настоящей заметке решена задача описания полугруппы (конечных), которые можно изоморфно представить как транзитивные или симметричные полугруппы преобразований. Этим самым получено также решение одной задачи теории автоматов, описанной ниже.

Пусть $\mathfrak{A}$ — автомат с множеством состояний S (под автоматом здесь можно понимать как автомат Мили или Мура, так и их обобщения, когда не требуется, чтобы полугруппа, образуемая входами автомата, была свободной). Каждое входное слово $\mathfrak{A}$ осуществляет некоторое преобразование множества S : совокупность всех таких преобразований является полугруппой преобразований. Эта полугруппа называется полугруппой автомата $\mathfrak{A}$ ($\cdot$). В случае, когда эта полугруппа транзитивна, автомат $\mathfrak{A}$ называется сильно связным (или простым) (¹). Если полугруппа автомата $\mathfrak{A}$ симметрична, автомат $\mathfrak{A}$ называется ядерным (или обратимым) (²). Если S конечно, то у автомата $\mathfrak{A}$ всегда существуют минимальные (по состояниям) подавтоматы, которые, как легко видеть, будут сильно связными. Объединение всех минимальных подавтоматов будет подавтоматом, который называется ядром автомата $\mathfrak{A}$. Ясно, что ядро будет ядерным автоматом. Таким образом, конечный автомат является ядерным в точности тогда, когда он совпадает со своим ядром.

Говорят, что автомат $\mathfrak{A}$ принадлежит полугруппе G , если G изоморфна полугруппе автомата $\mathfrak{A}$ (⁴). В этой заметке нами описаны полугруппы, которым принадлежат конечные сильно связные и конечные ядерные автоматы. Заметим, что аналогичные задачи для частичных автоматов (т. е. автоматов, у которых функция переходов не обязательно всюду определена) в конечном и бесконечном случае решена в нашей работе (²) (в теоретико-полугрупповой формулировке).

Предварительно введем некоторые определения. Наименьший двусторонний идеал полугруппы G (если он существует) называется ядром G . Ясно, что у конечной полугруппы ядро существует всегда. Подмножество H полугруппы G называется левым редуктором (или леворедуктивным) (³), если для любых $a, b \in G$ из того, что для всех $h \in H$ $ha = hb$, следует, что $a = b$. Идемпотент i полугруппы G называется примитивным, если он не является нулем G и для любого ненулевого идемпотента $j \in G$ из $j = ij = ji$ следует, что $i = j$.

Пусть Γ — конечная группа, $0 \notin \Gamma$, n — натуральное число. Матрица размерности $n \times n$, в каждой строке которой стоит в точности один элемент из Γ , а все остальные элементы равны 0, называется строчно-

мономимальной матрицей над Γ . Если положить $0\gamma = \gamma 0 = 0$ и $0 + \gamma = \gamma + 0 = \gamma$ для всех $\gamma \in \Gamma \cup \{0\}$, то строчно-мономимальные матрицы одинаковой размерности можно перемножать обычным образом, причем операция умножения будет ассоциативной, а произведение строчно-мономимальных матриц снова будет строчно-мономимальной матрицей. Поэтому можно рассматривать полугруппы (не обязательно всех) строчно-мономимальных матриц данной размерности над данной группой. Полугруппа строчно-мономимальных матриц называется *эффективной*, если для любых натуральных i и j , меньших n (где $n \times n$ — размерность матриц); она содержит матрицу, в которой на пересечении i -й строки и j -го столбца стоит элемент, отличный от 0 (т. е. все матрицы нашей полугруппы не могут содержать 0 на некотором фиксированном месте).

Основным результатом заметки является:

Теорема. Для конечной полугруппы G следующие условия эквивалентны:

- 1) G изоморфна транзитивной полугруппе преобразований;
- 2) G разлагается в подпрямое произведение полугрупп, каждая из которых изоморфна транзитивной полугруппе преобразований;
- 3) G изоморфна симметричной полугруппе преобразований;
- 4) полугруппе G принадлежит некоторый конечный сильно связный автомат;
- 5) полугруппе G принадлежит некоторый конечный ядерный автомат;
- 6) пусть $a, b, c \in G$; если для любого $x \in G$ существует такое натуральное n , что $(cx)^na = (cx)^nb$, то $a = b$;
- 7) все правые идеалы полугруппы G леворедуктивны;
- 8) все минимальные правые идеалы полугруппы G леворедуктивны;
- 9) множество всех идемпотентов любого минимального правого идеала полугруппы G леворедуктивно;
- 10) ядро полугруппы G леворедуктивно;
- 11) полугруппа G не содержит нуля и множество примитивных идемпотентов G леворедуктивно;
- 12) G изоморфна некоторой допустимой полугруппе строчно-мономимальных матриц.

Замечание. Если конечная полугруппа G изоморфна транзитивной (симметричной) полугруппе преобразований множества A , то A является (может быть выбрано) конечным. Мы не считаем пустое слово входным словом автомата; в противном случае полугруппа автомата всегда содержит тождественное преобразование и в условиях 4) и 5) теоремы вместо G следует подставить полугруппу G^1 , получающуюся из G в результате присоединения единицы (если G уже не обладает единицей).

Доказательство. Пусть G — произвольная (не обязательно конечная) полугруппа. Импликация 1) $\rightarrow$ 2) очевидна, эквивалентность 2) $\leftrightarrow$ 3) была доказана в работе (*), эквивалентности 1) $\leftrightarrow$ 4) и 3) $\leftrightarrow$ 5) следуют из определений (в случае конечных автоматов и G следует рассматривать конечной). Дальнейшее доказательство состоит в проверке цепи импликаций.

3) $\rightarrow$ 6). Пусть P — изоморфизм G на симметричную полугруппу преобразований множества A и для любого $x \in G$ существует такое n , что $(cx)^na = (cx)^nb$. Пусть $P(a)(\alpha) = \beta$, $P(c)(\alpha) = \gamma$, где $\alpha, \beta, \gamma \in A$. Поскольку образ G при изоморфизме P симметричен, найдется $x \in G$, для которого $P(x)(\gamma) = \alpha$. Следовательно, $P(cx)(\alpha) = (P(x) \circ P(c))(\alpha) = P(x)(P(c)(\alpha)) = P(x)(\gamma) = \alpha$. Заметим, что произведение преобразований мы записываем справа налево, так что $P(cx) = P(x) \circ P(c)$ для любых $s, x \in G$. Таким образом, $P((cx)^n)(\alpha) = \alpha$ для любого n . Поэтому $P((cx)^nb)(\alpha) = P((cx)^na)(\alpha) = P(a)(P((cx)^n)(\alpha)) = P(a)(\alpha) = \beta$. С другой стороны, $\beta = P((cx)^nb)(\alpha) = P(b)(P((cx)^n)(\alpha)) = P(b)(\alpha)$, по-

этому $P(a)(a) = P(b)(a)$. Так как это верно для любого $a \in A$, $P(a) = P(b)$, а поскольку P — изоморфизм, то $a = b$.

6) $\rightarrow$ 7). Пусть I — правый идеал G и $ya = ab$ для всех $y \in I$. Если $c \in I$, то $cx \in I$ для всех $x \in G$, следовательно, $(cx)a = (cx)b$. По условию 6), $a = b$, т. е. I — левый редуктор.

Импликация 7) $\rightarrow$ 8) тривиальна.

8) $\rightarrow$ 9). При доказательстве предположим, что G периодична (т. е. каждый элемент G порождает конечную подполугруппу). Пусть I — минимальный правый идеал G и E — множество его идемпотентов, пусть $ia = ib$ для всех $i \in E$. Если $c \in I$, то из периодичности G следует, что некоторая степень c , например, c^n , является идемпотентом. $c^n G$ — правый идеал, содержащийся в I , так что $c^n G = I$, значит, $c \in c^n G$, т. е. $c = c^n x$ для некоторого $x \in G$. Поэтому $c^{n+1} = (c^n \cdot c^n)x = c^n x = c$ и $ca = c(c^n a) = c(c^n b) = cb$ для всех $c \in I$. Так как I — левый редуктор, $a = b$.

Импликация 9) $\rightarrow$ 10) следует из того, что всякий минимальный правый идеал содержится в ядре полугруппы и что всякое подмножество, содержащее левый редуктор, само леворедуктивно.

Импликация 10) $\rightarrow$ 11) доказывается точно так же, как 8) $\rightarrow$ 9), если учесть, что ядро конечной полугруппы без нуля есть вполне простая полугруппа, а примитивные идемпотенты — в точности идемпотенты ядра (⁵).

11) $\rightarrow$ 12). Допустим, что G конечна. Поскольку примитивные идемпотенты G принадлежат ядру K полугруппы G , получаем, что выполняется условие 10). Каждому $g \in G$ поставим в соответствие преобразование ρ^g ядра K : $\rho^g(k) = kg$ для всех $k \in K$. Легко проверить, что $\rho^a \circ \rho^b = \rho^{ab}$ для любых $a, b \in G$. Левая редуктивность K означает, что $\rho^a = \rho^b \rightarrow a = b$, т. е. отображение ρ : $a \rightarrow \rho^a$ есть изоморфизм. Преобразование φ полугруппы S называется ее правым сдвигом, если $\varphi(st) = s\varphi(t)$ для любых $s, t \in S$. Из $\rho^s(ab) = abg = a\rho^s(b)$ следует, что ρ^s — правый сдвиг. Известно (^{6, 7}), что полугруппа всех правых сдвигов вполне простой полугруппы (какой является K) изоморфна полугруппе всех строчно-мономиальных матриц фиксированной конечной размерности над некоторой конечной группой, поэтому G изоморфна некоторой полугруппе строчно-мономиальных матриц. При этом полугруппе K соответствуют матрицы, в которых все элементы некоторого столбца отличны от 0 (и, следовательно, все остальные элементы равны 0), причем в качестве образов элементов из K встречаются матрицы, в которых любой наперед заданный столбец содержит отличные от 0 элементы (отображение K в полугруппу матриц является представлением Шютцманберже (⁷)). Поэтому G изоморфна эффективной полугруппе строчно-мономиальных матриц.

12) $\rightarrow$ 1). Без ущерба для общности можно предположить, что G есть эффективная полугруппа строчно-мономиальных матриц размерности $n \times n$ над некоторой конечной группой Γ . Элемент, стоящий на пересечении i -й строки и j -го столбца матрицы g , обозначим через g_{ij} . Пусть $(cx)a = (cx)b$ для всех $x \in G$ и некоторых $a, b, c \in G$. Допустим, что $a_{ij} \in \Gamma$ и $c_{ik} \in \Gamma$. В силу эффективности G , найдется матрица x такая, что $x_{ki} \in \Gamma$. Поэтому $(cxb)_{ij} = (cxa)_{ij} = c_{ik}x_{ki}a_{ij} \in \Gamma$. Отсюда, в силу строчной мономиальности матриц, $b_{ij} = a_{ij}$. Поэтому $a = b$. Таким образом, идеал cG полугруппы G леворедуктивен. Поскольку G конечна, она имеет минимальный правый идеал, скажем, I . Если $c \in I$, то $cG \subset I$, откуда следует, что I леворедуктивен. Каждому $g \in G$ поставим в соответствие преобразование ρ^g идеала I : $\rho^g(i) = ig$ для любого $i \in I$. Поскольку I — правый идеал, $i \in I$ влечет $\rho^g(i) \in I$. Пользуясь левой редуктивностью I , без труда проверяем, что соответствие ρ : $g \rightarrow \rho^g$ есть изоморфизм. Пусть $i_1, i_2 \in I$. Тогда $i_1 G$ есть правый идеал G , содержащийся в I , откуда $i_1 G = I$. Поэтому $i_2 \in i_1 G$, т. е. $i_2 = i_1 x$ для некоторого $x \in G$. Следо-

вательно, $\rho^*(i_i) = i_i$, т. е. образ G при изоморфизме ρ — транзитивная полугруппа преобразований. Теорема доказана. $(1) \leftrightarrow (8)$ было доказано в работе ⁽⁸⁾.

Без труда получаем, что конечные полугруппы G , описанные в теореме, не могут иметь левого нуля (и, в частности, нуля), если они содержат более одного элемента; идемпотенты таких полугрупп не могут попарно коммутировать при умножении (за исключением случая, когда G содержит единственный идемпотент, т. е. является группой), в частности, если G — не группа, то G не может быть и инверсной полугруппой.

Саратовский государственный университет
им. Н. Г. Чернышевского

Поступило
12 XI 1971

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

- ¹ В. М. Глушков, УМН, 16, № 5, 3 (1961). ² В. М. Schein, Dissertationes Mathematicae, 77, 1 (1970). ³ G. Thierrin, Comm. Math. Helv., 31, № 2, 145 (1956). ⁴ Б. М. Шайн, УМН, 18, № 3, 215 (1963). ⁵ Е. С. Ляпин, Полугруппы, М., 1960. ⁶ A. H. Clifford, Trans. Am. Math. Soc., 68, № 2, 165 (1950). ⁷ A. H. Clifford, G. B. Preston, The Algebraic Theory of Semigroups, 1, Providence, 1961. ⁸ E. J. Tully jr., Am. J. Math., 83, № 3, 533 (1961); ibid., 84, 386 (1962).