АВТОМАТЫ И ПОЛУГРУППЫ. II

И. ПЕАК (Сегед)*

Результаты настоящей заметки примыкают к исследованиям, приведенным в работах А. К. Флекка [1] и Р. Х. Ёмке [3].

Автоматом называется объект $A=(\mathfrak{A},\mathfrak{X},\delta)$, состоящий из двух непустых множеств $\mathfrak{A}, \mathfrak{X}$ и функции $\delta:\mathfrak{A}\times\mathfrak{X}\to\mathfrak{A}$. Для произвольного состояния $a(\in\mathfrak{A})$ и произвольного слова $p=x_1x_2\ldots x_k$ $(\in F(\mathfrak{X}))$[1] мы полагаем $ap=a_k$ $(\in\mathfrak{A})$, если $\delta(a,x_1)=a_1$, $\delta(a_1,x_2)=a_2$, ..., $\delta(a_{k-1},x_k)=a_k$. Автомат $A=(\mathfrak{A},\mathfrak{X},\delta)$ называется коммутативным, если для произвольных $a(\in\mathfrak{A})$, p, q $(\in F(\mathfrak{X}))$ имеет место $apq=aqp$. Состояние $a_0(\in\mathfrak{A})$ автомата $A=(\mathfrak{A},\mathfrak{X},\delta)$ мы назовем образующим элементом автомата A, если для каждого $a(\in\mathfrak{A})$ существует слово $p(\in F(\mathfrak{X}))$ так, что $a=a_0p$. Автомат называется циклическим, если он имеет образующий элемент, и — сильно связным, если каждое его состояние является образующим элементом этого автомата.

Пусть задан произвольный автомат $A=(\mathfrak{A},\mathfrak{X},\delta)$. Через $E(A)$ мы условимся обозначать полугруппу всех эндоморфизмов автомата A, т. е. множество всех однозначных отображений η: $\mathfrak{A}\to\mathfrak{A}$, удовлетворяющих условию $\eta(\delta(a,x))=\delta(\eta(a),x)$ $(a\in\mathfrak{A}; x\in\mathfrak{X})$, если в этом множестве произведение понимается в обычном смысле, как произведение отображений. Если эндоморфизм $\eta(\in E(A))$ является взаимно однозначным отображением множества $\mathfrak{A}$ на себя, то η называется автоморфизмом автомата A. Группа всех автоморфизмов автомата A обозначается через $G(A)$. Следуя В. М. Глушкову [2], каждому автомату $A=(\mathfrak{A},\mathfrak{X},\delta)$ мы сопоставляем полугруппу $S(A)$, определенную как фактор-полугруппа $F(\mathfrak{X})/\varrho(A)$ свободной полугруппы $F(\mathfrak{X})$ без единицы в алфавите $\mathfrak{X}$ по отношению конгруентности

$$p\equiv q(\varrho(A))\Leftrightarrow \underset{a\in\mathfrak{A}}{\forall}\, a[ap=aq]\quad (p,q\in F(\mathfrak{X})),$$

индуцируемому автоматом A.[2])

Естественным образом возникает вопрос о том, какие связи можно установить между некоторым автоматом A, с одной стороны, и принадлежащими ему полугруппами $S(A)$, $E(A)$ и группой $G(A)$, — с другой.

В работе А. К. Флекка [1] рассматриваются коммутативные сильно связные автоматы и устанавливаются некоторые связи между такими авто-

---

* I. Peák (Szeged)

[1]) Через $F(\mathfrak{X})$ обозначается свободная полугруппа без единицы в алфавите $\mathfrak{X}$.

[2]) Относительно дальнейших определений мы ссылаемся на работы [2] и [4].

матами и их группами автоморфизмов.[3]) Настоящая заметка посвящена изучению коммутативных циклических автоматов. Нижеследующие результаты обобщают некоторые результаты работы А. К. Флекка [1], продолжают исследование, приведенное в работе Р. Х. Ёмке [3] и показывают, что *в алгебраической теории коммутативных циклических автоматов полугруппа эндоморфизмов играет аналогичную роль, как группа автоморфизмов — в теории коммутативных сильно связных автоматов.*

Теорема 1. *Если коммутативный автомат $A=(\mathfrak{A}, \mathfrak{X}, \delta)$ является циклическим, то полугруппы $S(A)$ и $E(A)$ будут изоморфными и имеет место $O(E(A))=|\mathfrak{A}|$* [4]).

Доказательство. Возьмем некоторый коммутативный циклический автомат $A=(\mathfrak{A}, \mathfrak{X}, \delta)$. Прежде всего мы покажем, что $O(S(A))=|\mathfrak{A}|$. Пусть $a_0(\in\mathfrak{A})$ является образующим элементом автомата A. Рассмотрим произвольное состояние $a\,(\in\mathfrak{A})$ и пусть $a=a_0p\ (p\in F(\mathfrak{X}))$. Если при этом $a=a_0p'$ $(p'\in F(\mathfrak{X}))$, то для каждого $b\,(\in\mathfrak{A})$ мы получим $bp=a_0rp=a_0pr=a_0p'r=$ $=a_0rp'=bp'$, где $b=a_0r\ (r\in F(\mathfrak{X}))$, т. е. $p\equiv p'(\varrho(A))$. Это означает, что можно определить однозначное отображение множества $\mathfrak{A}$ в полугруппу $S(A)$: $a\to C[p]\ \ (a\in\mathfrak{A},\ p\in F(\mathfrak{X}),\ a=a_0p)$. Ясно, что это отображение отображает множество $\mathfrak{A}$ на полугруппу $S(A)$ и легко убедиться, что оно будет взаимно однозначным. Следовательно, мы получили, что $O(S(A))=|\mathfrak{A}|$.

Далее, так как автомат A является коммутативным, то для каждого слова $p\ (\in F(\mathfrak{X}))$ отображение $\eta_p\colon a\to ap\ \ (a\in\mathfrak{A})$ будет эндоморфизмом автомата A и $\eta_p=\eta_q\Leftrightarrow p\equiv q(\varrho(A))\ (p, q\in F(\mathfrak{X}))$. Легко получается, что отображение $C[p]\to\eta_p$ является изоморфным отображением полугруппы $S(A)$ в полугруппу $E(A)$.

Осталось еще убедиться в том, что отображение $C[p]\to\eta_p$ отображает полугруппу $S(A)$ на полугруппу $E(A)$. Для этой цели мы покажем, что для каждого эндоморфизма $\eta(\in E(A))$ найдется слово $p(\in F(\mathfrak{X}))$, для которого имеет место $\eta=\eta_p$. Действительно, если $\eta(a_0)=a$ и $a=a_0p\ \ (p\in F(\mathfrak{X}))$, то для произвольного состояния $b(=a_0r;\ r\in F(\mathfrak{X}))$ мы получаем $\eta(b)=$ $=\eta(a_0r)=\eta(a_0)r=ar=a_0pr=a_0rp=bp$, т. е. имеет место $\eta=\eta_p$. Этим теорема 1 полностью доказана.[5])

Из теоремы 1 и из следствия теоремы 4 Флекка [1] мы получим, что *каждый эндоморфизм произвольного коммутативного сильно связного автомата является автоморфизмом.*

Мы заметим, что из того, что для некоторого коммутативного автомата A имеет место $S(A)\approx E(A)$, не следует, что автомат A будет циклическим.

---

[3]) В упомянутой работе А. К. Флекк рассматривает автомат в некотором обобщенном смысле.

[4]) $O(S)$ обозначает порядок полугруппы S, а $|\mathfrak{A}|$ — мощность множества $\mathfrak{A}$.

[5]) В другой формулировке, как Б. Чакань обратил внимание автора, эта теорема по существу означает, что в одном из результатов Флекка [1], согласно которому произвольная коммутативная и транзитивная полугруппа отображений некоторого множества в себя совпадает со своим централизатором в полугруппе всех отображений данного множества в себя, предположение о транзитивности может быть ослаблено. При таком подходе теорема 2 получается в качестве частного случая теоремы 1.

Действительно, коммутативный автомат

	0	1	2	3	4
x	1	2	0	4	3

удовлетворяет этому условию, но не является циклическим.

С другой стороны, существует автомат $A=(\mathfrak{A}, \mathfrak{X}, \delta)$, порядок полугруппы $E(A)$ которого равен мощности множества $\mathfrak{A}$, но он не является циклическим. Таким автоматом будет например автомат

	0	1
x	1	1

.

Возникает также вопрос о том, существует ли коммутативный автомат A, удовлетворяющий одновременно условиям $S(A)\approx E(A)$ и $O(E(A))=|\mathfrak{A}|$, который не является циклическим.

Как следующий пример покажет, ответ на этот вопрос является положительным. Действительно, коммутативный нециклический автомат A, заданный таблицей переходов

	0	1	2	3
x	0	1	2	3
y	1	0	2	3
z	0	1	3	2

удовлетворяет одновременно данным двум условиям. Далее, легко убедиться и в том, что для этого автомата A имеет место $E(A)\approx G(A)$. Этим доказано также, что то утверждение Флекка [1], обобщением которого является теорема 1 и согласно которому, если коммутативный автомат $A=(\mathfrak{A}, \mathfrak{X}, \delta)$ сильно связен, то имеют место соотношения $G(A)\approx S(A)$ и $O(G(A))=|\mathfrak{A}|$, оказывается необратимым.

Теорема 2. *Пусть циклический автомат A имеет n состояний. Если полугруппа $E(A)$ коммутативна и $O(E(A))=n$, тогда автомат A также является коммутативным.*

Доказательство. Рассмотрим циклический автомат $A=(\mathfrak{A}, \mathfrak{X}, \delta)$ с образующим элементом $a_0(\in\mathfrak{A})$, возьмем произвольный эндоморфизм $\eta\in E(A)$ и определим отображение $\eta\to\eta(a_0)$ полугруппы $E(A)$ в $\mathfrak{A}$. Легко убедиться, что это отображение будет взаимно однозначным и из-за $O(E(A))=n$ оно отображает полугруппу $E(A)$ на множество $\mathfrak{A}$. Следовательно, для каждого $a\ (\in\mathfrak{A})$ найдется $\eta(\in E(A))$, такое, что $\eta(a_0)=a$.

Предположим теперь, что автомат A не является коммутативным. Тогда существуют $a\ (\in\mathfrak{A})$ и $p, q\ (\in F(\mathfrak{X}))$, для которых $apq\neq aqp$. Возьмем тот эндоморфизм $\eta\ (\in E(A))$, для которого $\eta(a_0)=a$. Тогда $\eta(a_0pq)=\eta(a_0)pq=apq$ и $\eta(a_0qp)=\eta(a_0)qp=aqp$. Отсюда из-за $apq\neq aqp$ мы получим $a_0pq\neq a_0qp$. Возьмем теперь эндоморфизмы $\eta_1, \eta_2(\in E(A))$, удовлетворяющие условиям $\eta_1(a_0)=a_0p$ и $\eta_2(a_0)=a_0q$. Тогда $\eta_1\eta_2(a_0)=\eta_1(\eta_2(a_0))=\eta_1(a_0q)=$

$=\eta_1(a_0)q=a_0qp$ и $\eta_2\eta_1(a_0)=\eta_2(\eta_1(a_0))=\eta_2(a_0p)=\eta_2(a_0)p=a_0qp$. Следовательно, $\eta_1\eta_2(a_0)\neq\eta_2\eta_1(a_0)$, что противоречит предположениям теоремы. Этим теорема 2 доказана.

Из теоремы 1 и из теоремы 3 работы [4] сразу вытекает справедливость следующего предложения.

Теорема 3. *Если конечный коммутативный циклический автомат A является прямым произведением автоматов $A_1, \ldots, A_n$, то и полугруппа $S(A)$ будет прямым произведением полугрупп $S(A_1), \ldots, S(A_n)$.*

Если рассматривать прямое произведение специального вида, а именно, — $\mathfrak{X}$-прямое произведение[6]), тогда без ограничения конечности можно высказать следующее предложение.

Теорема 4. *Коммутативный циклический автомат A является $\mathfrak{X}$-прямым произведением автоматов тогда и только тогда, если полугруппа $S(A)$ является прямым произведением полугрупп.*

Доказательство этой теоремы получается при помощи модификации доказательства теоремы 6 из работы А. К. Флекка [1].

Действительно, рассмотрим коммутативный циклический автомат $A=(\mathfrak{A}, \mathfrak{X}, \delta)$ с образующим элементом $a_0(\in\mathfrak{A})$, полугуппа $S(A)$ которого является прямым произведением полугрупп. Тогда по теореме 1 мы имеем $S(A)\approx E(A)$ и $E(A)$ тоже является прямым произведением некоторых полугрупп S_1 и S_2, т. е. $E(A)\approx S_1\otimes S_2$. Без ограничения общности мы можем отождествить полугруппы $E(A)$ и $S_1\otimes S_2$. Возьмем теперь автомат $A_1=(S_1, \mathfrak{X}, \delta_1)$, функция переходов δ_1 которого определяется следующим образом: Для s_1 $(\in S_1)$ и x $(\in\mathfrak{X})$ мы полагаем $\delta_1(s_1, x)=s_1x_1(\in S_1)$, где $x_1(\in S_1)$ является первой компонентой эндоморфизма $\eta_x(\in E(A); a\to\delta(a, x))$ в прямом разложении $E(A)\approx S_1\otimes S_2$. Таким же образом определяется автомат $A_2=(S_2, \mathfrak{X}, \delta_2)$.

Достаточно еще показать, что автомат $A'=(S_1\times S_2, \mathfrak{X}, \delta')$, являющийся $\mathfrak{X}$-прямым произведением автоматов A_1 и A_2, изоморфен исходному автомату A. Легко убедиться, что искомым изоморфизмом может служить отображение $\varphi\colon S_1\times S_2\to\mathfrak{A}$, сопоставляющее каждому состоянию (s_1, s_2) автомата A' состояние a автомата A, являющееся образом образующего элемента a_0 $(\in\mathfrak{A})$ при эндоморфизме (s_1, s_2) $(\in S_1\otimes S_2)$. Действительно, по теореме 1 отображение φ является взаимно однозначным отображениием множества $S_1\times S_2$ на множество $\mathfrak{A}$. С другой стороны, мы имеем $\varphi(\delta'((s_1, s_2), x))=\varphi((\delta_1(s_1, x), \delta_2(s_2, x)))=\varphi((s_1x_1, s_2x_2))=\varphi((s_1, s_2)(x_1, x_2))=$ $=\varphi((s_1, s_2)\eta_x)=((s_1, s_2)\eta_x)(a_0)=\eta_x((s_1, s_2)(a_0))=\eta_x(\varphi(s_1, s_2))=\delta(\varphi((s_1, s_2)), x)$.

Пусть наоборот предполагается, что коммутативный циклический автомат $A=(\mathfrak{A}, \mathfrak{X}, \delta)$ является $\mathfrak{X}$-прямым произведением автоматов $A_1=(\mathfrak{A}_1, \mathfrak{X}, \delta_1)$ и $A_2=(\mathfrak{A}_2, \mathfrak{X}, \delta_2)$. Ясно,что тогда автоматы A_1 и A_2 также являются комму-

---

[6]) Мы говорим, что автомат $A=(\mathfrak{A}, \mathfrak{X}, \delta)$ является $\mathfrak{X}$-прямым произведением автоматов $A_i=(\mathfrak{A}_i, \mathfrak{X}, \delta_i)$ $(i=1, \ldots, n)$, если A изоморфен автомату $A'=(\mathfrak{A}', \mathfrak{X}, \delta')$, у которого $\mathfrak{A}'=\mathfrak{A}_1\times\ldots\times\mathfrak{A}_n$ и функция δ' определяется следующим образом: $\delta'((a_1, \ldots, a_n), x)=$ $=(\delta_1(a_1, x), \ldots, \delta_n(a_n, x))$ $(a_i\in\mathfrak{A}_i, x\in\mathfrak{X})$.

тативными и циклическими. Пусть a_0 $(\in \mathfrak{A})$ есть образующий элемент автомата A. Если отождествить автомат A с автоматом $A' = (\mathfrak{A}_1 \times \mathfrak{A}_2, \mathfrak{X}, \delta')$, являющимся $\mathfrak{X}$-прямым произведением автоматов A_1 и A_2, то состояния $a_0^{(1)} (\in \mathfrak{A}_1)$ и $a_0^{(2)} (\in \mathfrak{A}_2)$, удовлетворяющие условию $a_0 = (a_0^{(1)}, a_0^{(2)})$, будут образующими элементами автоматов A_1 и A_2, соответственно. Определим теперь следующее отображение: Каждому элементу $C[p]$ $(p \in F(\mathfrak{X}))$ полугруппы $S(A)$ мы сопоставляем тот элемент $(C_1[p_1], C_2[p_2])$ $(p_1, p_2 \in F(\mathfrak{X}))$ прямого произведения $S(A_1) \otimes S(A_2)$, для которого имеет место $a_0^{(1)} p_1 = a_1$, $a_0^{(2)} p_2 = a_2$ и $a_0 p = (a_1, a_2)$ $(a_i \in \mathfrak{A}_i)$. Не трудно убедиться, что это отображение является изоморфным отображением полугруппы $S(A)$ на полугруппу $S(A_1) \otimes S(A_2)$. Теорема доказана.

Исследуя взаимосвязь между автоматами и принадлежащими им группами автоморфизмов и полугруппами эндоморфизмов, естественным образом возникает вопрос о том, можно ли произвольную группу и произвольную полугруппу с единицей интерпретировать как группу автоморфизмов и полугруппу эндоморфизмов некоторого автомата, соответственно.

Теорема 4 Флекка [1] и теорема 1 настоящей заметки позволяют дать положительный ответ на этот вопрос в коммутативном случае.

Известно, что для каждой полугруппы S существует автомат A, полугруппа $S(A)$ которого изоморфна полугруппе S. Если например полугруппа S содержит единичный элемент, тогда такой автомат можно сконструировать следующим образом. Пусть X обозначает некоторую систему образующих элементов исходной полугруппы S. Возьмем произвольное множество $\mathfrak{A}$, мощность которого совпадает порядком полугруппы S и — множество $\mathfrak{X}$, мощность которого равна мощности множества X. Рассмотрим наконец взаимно однозначные отображения $f: \mathfrak{A} \to S$ множества $\mathfrak{A}$ на S и $g: \mathfrak{A} \to X$ множества $\mathfrak{X}$ на X, соответственно. Не трудно убедиться, что для автомата $A_S = (\mathfrak{A}, \mathfrak{X}, \delta)$, у которого функция переходов δ определяется формулой $\delta(a, x) = f^{-1}(f(a)g(x))$ $(a \in \mathfrak{A}; x \in \mathfrak{X})$, имеет место $S(A_S) \approx S$.

Используя эту конструкцию, доказывается следующая

Теорема 5. *Для каждой абелевой группы G существует автомат A, группа автоморфизмов $G(A)$ которого изоморфна заданной группе G. Далее, для каждой коммутативной полугруппы S с единицей найдется автомат A, полугруппа эндоморфизмов $E(A)$ которого изоморфна заданной полугруппе S.*

Доказательство. Действительно, рассмотрим произвольную абелеву группу G и (при некоторой системе образующих) сконструируем автомат A_G. Легко видеть, что автомат A_G будет коммутативным и сильно связным. Следовательно, из-за $S(A_G) \approx G$ из теоремы 4 Флекка [1] получается $G(A_G) \approx G$.

Далее, если задана произвольная коммутативная полугруппа S с единицей e, то автомат A_S (при произвольно выбранной системе образующих) будет коммутативным и циклическим. (Его образующим элементом может служить например прообраз единичного элемента e полугруппы S при отображении f.) Следовательно, из $S(A_S) \approx S$ и из теоремы 1 мы получим, $E(A_S) \approx S$, что и требовалось доказать.

Литература

[1] A. C. Fleck, Isomorphism groups of automata, *J. Assoc. Comp. Machinery*, **9** (1962), 469–476.
[2] В. М. Глушков, Абстрактная теория автоматов, *Успехи матем. наук*, **16:5 (101)** (1961), 3–62.
[3] R. H. Oehmke, On the structures of an automaton and its input semigroup, *J. Assoc. Comp. Machinery*, **10** (1963), 521–525.
[4] И. Пеак, Автоматы и полугруппы. I, *Acta Sci. Math.*, **25** (1964), 193–201.

(Поступило 26/X, 1964)