Группы автоморфизмов сильно связных автоматов

Ю.Н. Горчинский

Изучается строение группы автоморфизмов сильно связного автомата в терминах его подгруппы. Доказывается теорема о представлении счетных групп группами автоморфизмов сильно связных перестановочных автоматов.

1. Введение

Под автоматом A мы будем иметь в виду автомат без выходов, т.е. тройку (X_A, S_A, δ_A), где X_A - входной алфавит, S_A - внутренний алфавит, $X_A \times S_A \xrightarrow{\delta_A} S_A$ - функция переходов. Преобразование $\delta_A^{(x)}$, $x \in X_A$ внутреннего алфавита $s^{\delta_A^{(x)}} = \delta_A(x, s)$, $s \in S_A$ называется частичной функцией переходов. Через $\Sigma(M)$ мы будем обозначать симметрическую группу множества M, а через $\overline{\Sigma}(M)$ - симметрическую полугруппу этого множества. Подполугруппа G_A, порожденная в $\overline{\Sigma}(S_A)$ множеством Ω_A всех частичных функций переходов, называется полугруппой автомата A. Если $\delta_A^{(x)}$, $x \in X_A$ - биективные преобразования, то автомат A называется перестановочным. В случае перестановочного автомата A его полугруппа является группой и называется группой автомата A. Автомат A называется сильно связным, если G_A - транзитивная полугруппа преобразований.

Будем называть автомат A вполне неавтономным, если из $x \neq x'$ следует $\delta_A^{(x)} \neq \delta_A^{(x')}$.

Автоморфизмом автомата A называется пара $\varphi_A = (\varphi_{X_A}, \varphi_{S_A})$ подстановок, где φ_{X_A} – подстановка входного алфавита, а φ_{S_A} - подстановка внутреннего алфавита, удовлетворяющая тождеству:

$$\delta_A(x^{\varphi_{X_A}}, s^{\varphi_{S_A}}) = (\delta_A(x,s))^{\varphi_{S_A}} \tag{1}$$

Можно смотреть на φ_A как на элемент группы $\Sigma(X_A) \times \Sigma(S_A)$ с компонентами φ_{X_A} и φ_{S_A} соответственно в прямых множителях $\Sigma(X_A)$ и $\Sigma(S_A)$. Тогда множество $\mathrm{Aut}\,A$ всех автоморфизмов автомата A является подгруппой группы $\Sigma(X_A) \times \Sigma(S_A)$. Мы будем называть группу $\mathrm{Aut}\,A$ группой автоморфизмов автомата A, а любую подгруппу группы $\mathrm{Aut}\,A$ - подгруппой автоморфизмов автомата A. Группы автоморфизмов автоматов играют известную роль в вопросах классификации автоматов.

В [1]-[3] изучалась подгруппа автоморфизмов $\mathrm{Aut}\,A \cap \Sigma(S_A)$ конечного сильно связного автомата A. При этом в [2]-[3] предполагалось, что X_A - полугруппа.

Настоящая статья состоит из четырех разделов.

В разделе 1 группы автоморфизмов автоматов сводятся к группам автоморфизмов вполне неавтономных автоматов. При этом сильная связность автомата сохраняется.

В разделе 2 для вполне неавтономного сильно связного автомата A описывается строение $\mathrm{Aut}\,A$ путем установления его связи с полугруппой G_A и ее группой автоморфизмов $\mathrm{Aut}\,G_A$.

В разделе 3 строение $\mathrm{Aut}\,A$ существенно упрощается в случае вполне неавтономного сильно связного перестановочного автомата A. Здесь оно связано с группой G_A и ее группой автоморфизмов $\mathrm{Aut}\,G_A$.

В разделе 4 доказывается, что любая счетная группа H изоморфна группе автоморфизмов некоторого конечного вполне неавтономного сильно связного перестановочного автомата A. При этом устанавливается связь между числом образующих группы H и $|X_A|$ в том случае, когда H - конечная группа.

2. Редукция к вполне неавтономным автоматам

Пусть A - произвольный автомат. Введем эквивалентность ξ_{X_A} на множестве X_A: $x \equiv x' \pmod{\xi_{X_A}}$ тогда и только тогда, когда

$\delta_A^{(x)} = \delta_A^{(x')}$. Легко видеть, что $\xi_A = (\xi_{X_A}, \Delta_{S_A})$, где Δ_{S_A} - эквивалентность на S_A с одноэлементными классами, будет конгруэнцией на автомате A. Положим $\overline{A} = A/\xi_A$. Определим эквивалентность $\delta_{X_{\overline{A}}}$ на множестве $X_{\overline{A}}$: тогда и только тогда $x^{\xi_{X_A}} \equiv x'^{\xi_{X_A}} \pmod{\delta_{X_A}}$, когда $|x^{\xi_{X_A}}| = |x'^{\xi_{X_A}}|$ ($|M|$ - мощность M). Классы эквивалентности ξ_{X_A} обозначим через $M_1, M_2, \ldots, M_d$, а классы эквивалентности $\delta_{X_{\overline{A}}}$ через $N_1, N_2, \ldots, N_t$. Очевидно, $\overline{A}$ - вполне неавтономный автомат, причем, если A - сильно связный, то и $\overline{A}$ - сильно связный.

Теорема 1. *Для произвольного автомата A группа* $\mathrm{Aut}\, A$ *является расширением группы $\Sigma(M_1) \times \Sigma(M_2) \times \cdots \times \Sigma(M_d)$ при помощи группы*

$$\mathrm{Aut}\, \overline{A} \cap (\Sigma(N_1) \times \Sigma(N_2) \times \cdots \times \Sigma(N_t) \times \Sigma(S_A)).$$

Доказательство. Пусть $\varphi_A \in \mathrm{Aut}\, A$, $\varphi_A = (\varphi_{X_A}, \varphi_{S_A})$. Определим преобразование $\varphi_{X_{A/\xi_{X_A}}}$ множества $X_{A/\xi_{X_A}}$:

$$(x^{\xi_{X_A}})^{\varphi_{X_A/\xi_{X_A}}} = (x^{\varphi_{X_A}})^{\xi_{X_A}}. \tag{2}$$

Определение (2) корректно, так как не зависит от представителей классов эквивалентности ξ_{X_A}. Действительно, если $x \equiv x' \pmod{\xi_{X_A}}$, то $\delta_A^{(x)} = \delta_A^{(x')}$ и, согласно (1), для любого $s \in S_A$

$$\delta_A(x^{\varphi_{X_A}}, s^{\varphi_{S_A}}) = (\delta_A(x, s))^{\varphi_{S_A}} = (\delta_A(x', s))^{\varphi_{S_A}} = \delta_A(x'^{\varphi_{X_A}}, s^{\varphi_{S_A}}),$$

откуда $\delta_A^{(x^{\varphi_{X_A}})} = \delta_A^{(x'^{\varphi_{X_A}})}$, т.е.

$$x^{\varphi_{X_A}} \equiv x'^{\varphi_{X_A}} \pmod{\xi_{X_A}}.$$

Пользуясь (2), определением $\delta_{\overline{A}}$ и тождеством (1), будем иметь:

$$\begin{aligned}&\delta_{\overline{A}}((x^{\xi_{X_A}})^{\varphi_{X_A/\xi_{X_A}}}, s^{\varphi_{S_A}}) = \delta_{\overline{A}}((x^{\varphi_{X_A}})^{\xi_{X_A}}, s^{\varphi_{S_A}}) = \\ &= \delta_A(x^{\varphi_{X_A}}, s^{\varphi_{S_A}}) = (\delta_A(x, s))^{\varphi_{S_A}} = (\delta_{\overline{A}}(x^{\xi_{X_A}}, s))^{\varphi_{S_A}}.\end{aligned}$$

Следовательно, полагая

$$\varphi_{\overline{A}} = (\varphi_{X_{A/\xi_{X_A}}}, \varphi_{S_A}), \tag{3}$$

получим:

$$\varphi_{\overline{A}} \in \mathrm{Aut}\, \overline{A}. \tag{4}$$

Ввиду (2) и (4) определено отображение $\mathrm{Aut}\,A \xrightarrow{\theta} \mathrm{Aut}\,\overline{A}$, при котором
$$\varphi_A^\theta = \varphi_{\overline{A}}, \quad \varphi_A \in \mathrm{Aut}\,A. \tag{5}$$

Из (4) и (5) следует:
$$\varphi_A^\theta \cdot \psi_A^\theta = (\varphi_{X_A/\xi_{X_A}} \cdot \psi_{X_A/\xi_{X_A}}, \varphi_{S_A} \cdot \psi_{S_A}). \tag{6}$$

С другой стороны, согласно (2), (3), (5),
$$(\varphi_A \cdot \psi_A)^\theta = (\chi_{X_A/\xi_{X_A}}, \varphi_{S_A} \cdot \psi_{S_A}), \tag{7}$$
где для любого $x \in X_A$
$$\left(x^{\xi_{X_A}}\right)^{\chi_{X_A/\xi_{X_A}}} = (x^{\varphi_{X_A}\cdot\psi_{X_A}})^{\xi_{X_A}}. \tag{8}$$

Но в соответствии с (2),
$$(x^{\varphi_{X_A}\cdot\psi_{X_A}})^{\xi_{X_A}} = \left((x^{\varphi_{X_A}})^{\xi_{X_A}}\right)^{\psi_{X_A/\xi_{X_A}}} = \left(x^{\xi_{X_A}}\right)^{\varphi_{X_A/\xi_{X_A}}\cdot\psi_{X_A/\xi_{X_A}}}.$$

Поэтому из (8) получаем:
$$\chi_{X_A/\xi_{X_A}} = \varphi_{X_A/\xi_{X_A}} \cdot \psi_{X_A/\xi_{X_A}}. \tag{9}$$

Принимая во внимание (9), заключаем на основании (7) и (6):
$$(\varphi_A \cdot \psi_A)^\theta = \varphi_A^\theta \cdot \psi_A^\theta, \quad \varphi_A, \psi_A \in \mathrm{Aut}\,A,$$
откуда следует, что θ - гомоморфизм группы $\mathrm{Aut}\,A$ в группу $\mathrm{Aut}\,\overline{A}$. Таким образом, по теореме о гомоморфизме групп, группа $\mathrm{Aut}\,A$ является расширением группы $\ker\theta$ при помощи группы $(\mathrm{Aut}\,A)^\theta$. Пусть $\varphi_A \in \ker\theta$, $\varphi_A = (\varphi_{X_A}, \varphi_{S_A})$. Тогда $\varphi_A^\theta = e_{\overline{A}}$, $e_{\overline{A}} = (e_{X_A/\xi_{X_A}}, e_{S_A/\xi_{S_A}})$, где $e_{X_A/\xi_{X_A}}$, $e_{S_A/\xi_{S_A}}$ - тождественные преобразования, соответственно X_A/ξ_{X_A} и S_A/ξ_{S_A}.

Отсюда, согласно (5) и (4), следует:
$$\left(x^{\xi_{X_A}}\right)^{\varphi_{X_A/\xi_{X_A}}} = x^{\xi_{X_A}}, \quad x \in X_A, \tag{10}$$
$$\varphi_{S_A} = e_{S_A}, \tag{11}$$
где e_{S_A} - тождественное преобразование S_A.

В силу (2), тождество (10) влечет за собой:

$$x^{\varphi_{X_A}} \equiv x \pmod{\xi_{X_A}}, \quad x \in X_A,$$

откуда

$$\varphi_{X_A} \in \Sigma(M_1) \times \Sigma(M_2) \times \cdots \times \Sigma(M_d). \tag{12}$$

Предположим теперь, что соотношения (11) и (12) выполнены. Тогда

$$\delta_A(x^{\varphi_{X_A}}, s^{\varphi_{S_A}}) = s^{\delta_A^{(x^{\varphi_{X_A}})}} = s^{\delta_A^{(x)}} = (\delta_A(x,s))^{\varphi_{S_A}}$$

и, следовательно, $\varphi_A \in \operatorname{Aut} A$. Кроме того, ввиду обратимости приведенных рассуждений, $\varphi_A^\theta = e_{\overline{A}}$. Таким образом, $\varphi_A \in \ker\theta$. Этим доказано, что

$$\ker\theta = \Sigma(M_1) \times \Sigma(M_2) \times \cdots \times \Sigma(M_d). \tag{13}$$

Пусть $(\varphi_{X_A/\xi_{X_A}}, \varphi_{S_A}) = \varphi_{\overline{A}} \in (\operatorname{Aut} A)^\theta$. Тогда имеет место (5) и потому (3), где $\varphi_A \in \operatorname{Aut} A$, $\varphi_A = (\varphi_{X_A}, \varphi_{S_A})$. В силу (2), отсюда следует, что $|x^{\xi_{X_A}}| = |(x^{\varphi_{X_A}})^{\xi_{X_A}}|$, $x \in X_A$. Поэтому $x^{\xi_{X_A}} \equiv (x^{\varphi_{X_A}})^{\xi_{X_A}} \pmod{\delta_{X_A}}$, $x \in X_A$. Обращаясь снова к (2), заключаем на основании последнего сравнения, что

$$\varphi_{X_A/\xi_{X_A}} \in \Sigma(N_1) \times \Sigma(N_2) \times \cdots \times \Sigma(N_t),$$

и, значит,

$$\varphi_{\overline{A}} \in \operatorname{Aut}\overline{A} \cap (\Sigma(N_1) \times \Sigma(N_2) \times \cdots \times \Sigma(N_t) \times \Sigma(S_A)). \tag{14}$$

Предположим теперь, что включение (14) имеет место. Тогда

$$|(x^{\xi_{X_A}})^{\varphi_{X_A/\xi_{X_A}}}| = |x^{\xi_{X_A}}|, \quad x \in X_A. \tag{15}$$

Ввиду (15), найдется $\varphi_{X_A} \in \Sigma(X_A)$,

$$(x^{\varphi_{X_A}})^{\xi_{X_A}} = (x^{\xi_{X_A}})^{\varphi_{X_A/\xi_{X_A}}}, \quad x \in X_A. \tag{16}$$

Так как, в силу (14), $\varphi_{\overline{A}} \in \operatorname{Aut}\overline{A}$, то, используя (16), получим:

$$\begin{aligned} \delta_A(x^{\varphi_{X_A}}, s^{\varphi_{S_A}}) &= \delta_{\overline{A}}((x^{\varphi_{X_A}})^{\xi_{X_A}}, s^{\varphi_{S_A}}) = \delta_{\overline{A}}((x^{\xi_{X_A}})^{\varphi_{X_A/\xi_{X_A}}}, s^{\varphi_{S_A}}) = \\ &= (\delta_{\overline{A}}(x^{\xi_{X_A}}, s))^{\varphi_{S_A}} = (\delta_A(x,s))^{\varphi_{S_A}}, \end{aligned}$$

откуда, согласно (1), $\varphi_A = (\varphi_{X_A}, \varphi_{S_A}) \in \operatorname{Aut} A$.

Поэтому из (16) следует: $\varphi_{\overline{A}} = \varphi_A^\theta$ и, значит, $\varphi_{\overline{A}} \in (\operatorname{Aut} A)^\theta$.

Этим доказано, что

$$(\operatorname{Aut} A)^\theta = \operatorname{Aut}\overline{A} \cap (\Sigma(N_1) \times \Sigma(N_2) \times \cdots \times \Sigma(N_t) \times \Sigma(S_A)). \tag{17}$$

Утверждение теоремы 1 теперь следует из равенств (13) и (17).

3. Строение группы автоморфизмов вполне неавтономного сильно связного автомата

Мы здесь будем пользоваться терминологией из книг [4] и [5]. Пусть A - вполне неавтономный сильно связный автомат, $\alpha \in S_A$.

Введем эквивалентность ρ_A на полугруппе G_A так, что $x \equiv y \pmod{\rho_A}$ тогда и только тогда, когда

$$\alpha^x = \alpha^y. \tag{18}$$

Очевидно, ρ_A - правая конгруэнция на G_A: для любого элемента $a \in G_A$ из (18) следует, что $\alpha^{xa} = \alpha^{ya}$.

Далее, в силу транзитивности G_A, для любых $a, b \in G_A$ найдется такой элемент $x \in G_A$, что $\alpha^{ax} = \alpha^b$. Поэтому произвольный элемент из G_A обратим справа по модулю ρ_A. Наконец, также из транзитивности G_A следует существование такого $e \in G_A$, что $\alpha^e = \alpha$, откуда $\alpha^{ex} = \alpha^x$, $x \in G$. Последнее тождество означает, что e - левая единица G_A по модулю ρ_A. Таким образом, правая конгруэнция ρ_A является модулярной.

Обозначим через $N_{G_A}(\rho_A)$ нормализатор правой конгруэнции ρ_A на G_A.

Положим:

$$N^{(e)}_{G_A}(\rho_A) = (a \in N_{G_A}(\rho_A) : \; ae \equiv a \pmod{\rho_A}),$$

$$M^{(e)}_{G_A}(\rho_A) = (c \in N^{(e)}_{G_A}(\rho_A) : \; \rho^c_A = \rho_A),$$

где ρ^c_A - правая конгруэнция, сопряженная с ρ_A [5].

Очевидно, $N^{(e)}_{G_A}(\rho_A)$ и $M^{(e)}_{G_A}(\rho_A)$ - подполугруппы полугруппы G_A. Для любого $\varphi \in \operatorname{Aut} G_A$ определим эквивалентность ρ^φ_A на G_A так, что $x^\varphi \equiv y^\varphi \pmod{\rho^\varphi_A}$ тогда и только тогда, когда $x \equiv y \pmod{\rho_A}$. Легко видеть, что ρ^φ_A является, как и ρ_A, модулярной правой конгруэнцией на G_A с условием обратимости справа по ее модулю произвольного элемента из G_A.

Пусть

$$\Phi_A = (\varphi \in \operatorname{Aut} G_A : \; \rho^\varphi_A = \rho^c, \; \exists c \in G_A).$$

Очевидно, что Φ_A - подгруппа группы $\mathrm{Aut}\, A$.

Стабилизатор множества M в группе подстановок H мы будем обозначать $(H)_M$, а множеств M_i, $i=\overline{1,l}$ - через $(H)_{M_i,\, i=\overline{1,l}}$.

Теорема 2. *Для произвольного вполне неавтономного сильно связного автомата A группа $\mathrm{Aut}\, A$ является расширением группы $M_{G_A}^{(e)}(\rho_A)\big/\rho_A\cap(M_{G_A}^{(e)}(\rho_A)\times M_{G_A}^{(e)}(\rho_A))$ при помощи группы $(\Phi_A)_{\Omega_A}$.*

Доказательство. Рассмотрим транзитивный модуль (S_A, G_A). Обозначим его группу автоморфизмов через $\mathrm{Aut}(S_A, G_A)$.

Пусть

$$(\varphi_{S_A}, \varphi_{G_A}) \in \mathrm{Aut}(S_A, G_A), \tag{19}$$

$$(\Omega_A)^{\varphi_{G_A}} = \Omega_A, \tag{20}$$

где $\varphi_{S_A} \in \Sigma(S_A)$, $\varphi_{G_A} \in \Sigma(G_A)$.

Ввиду (20), для любого $x \in X_A$ найдется $x' \in X_A$, так что

$$(\delta_A^{(x)})^{\varphi_{G_A}} = \delta_A^{(x')}. \tag{21}$$

Так как, в силу вполне неавтономности A, x' в правой части (21) определяется при заданном x однозначно, мы можем определить преобразование φ_{X_A} множества X_A, полагая

$$x^{\varphi_{X_A}} = x', \quad x \in X_A. \tag{22}$$

Из (20), (21) и (22) следует, что $\varphi_{X_A} \in \Sigma(X_A)$.

Далее, в силу (19) и (21)-(22),

$$\begin{aligned}\delta_A(x^{\varphi_{X_A}}, s^{\varphi_{S_A}}) &= (s^{\varphi_{S_A}})^{\delta_A^{(x^{\varphi_{X_A}})}} = (s^{\varphi_{S_A}})^{(\delta_A^{(x)})^{\varphi_{G_A}}} = \\ &= (s^{\delta_A^{(x)}})^{\varphi_{S_A}} = (\delta_A(x,s))^{\varphi_{S_A}},\end{aligned}$$

т.е. имеет место тождество (1).

Поэтому

$$(\varphi_{X_A}, \varphi_{S_A}) \in \mathrm{Aut}\, A \tag{23}$$

Таким образом, из (19)-(20) следует (23), где φ_{X_A} определено в (21) и (22).

Пусть теперь, наоборот, имеет место включение (23).

Так как Ω_A - система образующих полугруппы G_A, то произвольный элемент $\delta \in G_A$ можно представить в виде:

$$\delta = \delta_A^{(x_1)} \cdot \delta_A^{(x_2)} \cdot \ldots \cdot \delta_A^{(x_k)}, \quad x_i \in X_A, \quad i = \overline{1,k}. \tag{24}$$

Положим:

$$\delta' = \delta_A^{(x_1)^{\varphi X_A}} \cdot \delta_A^{(x_2)^{\varphi X_A}} \cdot \ldots \cdot \delta_A^{(x_k)^{\varphi X_A}}. \tag{25}$$

Ввиду (23), выполнено тождество (1), поэтому

$$s^{\varphi_{S_A} \cdot \delta_A^{(x^{\varphi X_A})}} = s^{\delta_A^{(x)} \cdot \varphi_{S_A}}, \quad s \in S_A, \quad x \in X_A,$$

откуда

$$\varphi_{S_A} \cdot \delta_A^{(x^{\varphi X_A})} = \delta_A^{(x)} \cdot \varphi_{S_A}, \quad x \in X_A. \tag{26}$$

Из (25) и (26) следует:

$$\varphi_{S_A} \cdot \delta' = \delta_A^{(x_1)} \cdot \delta_A^{(x_2)} \cdot \ldots \cdot \delta_A^{(x_k)} \cdot \varphi_{S_A},$$

т.е., согласно (24),

$$\varphi_{S_A} \cdot \delta' = \delta \cdot \varphi_{S_A}. \tag{27}$$

В силу (27)

$$(s^{\varphi_{S_A}})^{\delta'} = (s^{\delta})^{\varphi_{S_A}}, \quad s \in S_A. \tag{28}$$

Тождество (28) показывает, что преобразование φ_{G_A} полугруппы G_A, при котором $\delta^{\varphi_{G_A}} = \delta'$, является однозначным, и что

$$(\varphi_{S_A}, \varphi_{G_A}) \in \mathrm{Aut}(S_A, G_A), \quad \Omega_A^{\varphi_{G_A}} = \Omega_A.$$

Таким образом, из (23) следует (19) и (20), причем из (24)-(25) следует (21)-(22). Этим доказано, что (19)-(20) равносильны (23), где φ_{X_A} и φ_{G_A} связаны посредством (21)-(22).

Заметим, что так как (19) влечет за собой включение $\varphi_{G_A} \in \mathrm{Aut}\, G_A$, то φ_{G_A} однозначно определяется преобразованием φ_{X_A}.

Поэтому отображение

$$(\varphi_{S_A}, \varphi_{G_A}) \xrightarrow{\mu} (\varphi_{X_A}, \varphi_{S_A}),$$

$$(\varphi_{S_A}, \varphi_{G_A}) \in (\mathrm{Aut}(S_A, G_A))_{S_A \times \Omega_A}$$

является биективным отображением $(\mathrm{Aut}(S_A, G_A))_{S_A\times\Omega_A}$ на $\mathrm{Aut}\,A$.

Кроме того, если

$$(\varphi'_{S_A}, \varphi'_{G_A}),\ (\varphi''_{S_A}, \varphi''_{G_A}) \in (\mathrm{Aut}(S_A, G_A))_{S_A\times\Omega_A},$$

то, согласно (21)-(22),

$$(\delta_A^{(x)})^{\varphi'_{G_A}\cdot\varphi''_{G_A}} = (\delta_A^{(x^{\varphi'_{X_A}})})^{\varphi''_{G_A}} = \delta_A^{(x^{\varphi'_{X_A}\cdot\varphi''_{X_A}})},$$

где

$$(\delta_A^{(x)})^{\varphi'_{G_A}} = \delta_A^{(x^{\varphi'_{X_A}})}, \quad (\delta_A^{(x)})^{\varphi''_{G_A}} = \delta_A^{(x^{\varphi''_{X_A}})}, \quad x \in X_A.$$

Поэтому

$$((\varphi'_{S_A}, \varphi'_{G_A})\cdot(\varphi''_{S_A}, \varphi''_{G_A}))^{\mu} = (\varphi'_{S_A}\cdot\varphi''_{S_A}, \varphi'_{G_A}\cdot\varphi''_{G_A})^{\mu} = (\varphi'_{X_A}\cdot\varphi''_{X_A}, \varphi'_{S_A}\cdot\varphi''_{S_A}) =$$
$$= (\varphi'_{X_A}, \varphi'_{S_A})\cdot(\varphi''_{X_A}, \varphi''_{S_A}) = (\varphi'_{S_A}, \varphi'_{G_A})^{\mu}\cdot(\varphi''_{S_A}, \varphi''_{G_A})^{\mu}.$$

Следовательно, μ - изоморфизм $(\mathrm{Aut}(S_A, G_A))_{S_A\times\Omega_A}$ на $\mathrm{Aut}\,A$ и, значит,

$$\mathrm{Aut}\,A \simeq (\mathrm{Aut}(S_A, G_A))_{S_A\times\Omega_A}. \tag{29}$$

С другой стороны, согласно [6], модуль (S_A, G_A) эквивалентен модулю $(G_A/\rho_A, G_A)$, где

$$(a^{\rho_A})^b = (a\cdot b)^{\rho_A}, \quad a, b \in G_A.$$

Отсюда следует:

$$(\mathrm{Aut}(S_A, G_A))_{S_A\times\Omega_A} \simeq (\mathrm{Aut}(G_A/\rho_A, G_A))_{(G_A/\rho_A)\times\Omega_A}. \tag{30}$$

Теперь, на основании (30), получаем из (29):

$$\mathrm{Aut}\,A \simeq (\mathrm{Aut}(G_A/\rho_A, G_A))_{(G_A/\rho_A)\times\Omega_A} \tag{31}$$

Пусть

$$(\varphi_{G_A/\rho_A}, \varphi_{G_A}) \in \mathrm{Aut}(G_A/\rho_A, G_A). \tag{32}$$

Пусть

$$\varphi_{G_A} \in \mathrm{Aut}\,G_A. \tag{33}$$

Определим отображение $G_A/\rho_A \xrightarrow{\psi} G_A/\rho_A^{\varphi_{G_A}}$ следующим образом:

$$(a^{\rho_A})^{\psi} = (a^{\varphi_{G_A}})^{\rho_A^{\varphi_{G_A}}}, \quad a \in G_A. \tag{34}$$

Из определения правой конгруэнции $\rho_A^{\varphi_{G_A}}$ на полугруппе G_A, в соответствии с (33), вытекает биективность отображения ψ. Далее, используя (34), (33) и определения модулей $(G_A/\rho_A, G_A)$, $(G_A/\rho_A^{\varphi_{G_A}}, G_A)$, будем иметь:

$$\left((a^{\rho_A})^{\psi}\right)^{b^{\varphi_{G_A}}} = \left((a^{\varphi_{G_A}})^{\rho_A^{\varphi_{G_A}}}\right)^{b^{\varphi_{G_A}}} = (a^{\varphi_{G_A}} \cdot b^{\varphi_{G_A}})^{\rho_A^{\varphi_{G_A}}} =$$
$$= ((a \cdot b)^{\varphi_{G_A}})^{\rho_A^{\varphi_{G_A}}} = ((a \cdot b)^{\rho_A})^{\psi} = \left((a^{\rho_A})^{b}\right)^{\psi},$$

откуда следует, что (ψ, φ_{G_A}) - изоморфизм модуля $(G_A/\rho_A, G_A)$ на модуль $(G_A/\rho_A^{\varphi_{G_A}}, G_A)$. Поэтому, учитывая (32), получаем, что

$$(\varphi_{G_A/\rho_A}, \varphi_{G_A})^{-1} \cdot (\psi, \varphi_{G_A}) = (\varphi^{-1}_{G_A/\rho_A} \cdot \psi, e_{G_A}),$$

где e_{G_A} - тождественное преобразование G_A, также изоморфизм модуля $(G_A/\rho_A, G_A)$ на модуль $(G_A/\rho_A^{\varphi_{G_A}}, G_A)$. Следовательно, модули $(G_A/\rho_A, G_A)$ и $(G_A/\rho_A^{\varphi_{G_A}}, G_A)$ являются эквивалентными.

Так как правые конгруэнции ρ_A и $\rho_A^{\varphi_{G_A}}$ - модулярные, то отсюда следует, согласно теореме 11.10 из [5], что они сопряжены, т.е.

$$\rho_A^{\varphi_{G_A}} = \rho_A^{c}, \quad \exists c \in G_A. \tag{35}$$

При этом из доказательства леммы 11.9 в [5] следует, что

$$(b^{\rho_A^{\varphi_{G_A}}})^{\psi^{-1} \cdot \varphi_{G_A/\rho_A}} = (c \cdot b)^{\rho_A}, \quad b \in G_A \tag{36}$$

при том же $c \in G_A$, что и в (35).

Но, ввиду (34), для любого $a \in G_A$

$$(a^{\rho_A})^{\varphi_{G_A/\rho_A}} = (a^{\rho_A})^{\psi \cdot (\psi^{-1} \varphi_{G_A/\rho_A})} = \left((a^{\varphi_{G_A}})^{\rho_A^{\varphi_{G_A}}}\right)^{\psi^{-1} \cdot \varphi_{G_A/\rho_A}}.$$

Поэтому, используя (36) при $b = a^{\varphi_{G_A}}$, получим :

$$(a^{\rho_A})^{\varphi_{G_A/\rho_A}} = (c \cdot a^{\varphi_{G_A}})^{\rho_A}, \quad a \in G_A. \tag{37}$$

Таким образом, из включения (2) следуют соотношения (33), (35), (37).

Пусть теперь эти соотношения выполнены.

Определим $G_A/\rho_A^{\varphi_{G_A}} \xrightarrow{\chi} G_A/\rho_A$ следующим образом

$$(b^{\rho_A^{\varphi_{G_A}}})^{\chi} = (c \cdot b)^{\rho_A}, \quad b \in G_A \tag{38}$$

при том же $c \in G_A$, что и в (35).

Согласно лемме 11.8 в [5], из (35) следует, что (χ, e_{G_A}) - изоморфизм модуля $(G_A/\rho_A^{\varphi_{G_A}}, G_A)$ на модуль $(G_A/\rho_A, G_A)$.

С другой стороны, выше было доказано при условии (33), что (ψ, φ_{G_A}) - изоморфизм модуля $(G_A/\rho_A, G_A)$ на модуль $(G_A/\rho_A^{\varphi_{G_A}}, G_A)$, где отображение ψ определено в (34).

Поэтому

$$(\psi \cdot \chi, \varphi_{G_A}) \in \mathrm{Aut}(G_A/\rho_A, G_A). \tag{39}$$

Но, используя (34), (38), (37), будем иметь:

$$(a^{\rho_A})^{\psi\cdot\chi} = \left((a^{\varphi_{G_A}})^{\rho_A^{\varphi_{G_A}}}\right)^{\chi} = (c \cdot a^{\varphi_{G_A}})^{\rho_A} = (a^{\rho_A})^{\varphi_{G_A/\rho_A}}, \quad a \in G_A.$$

Следовательно,

$$\psi \cdot \chi = \varphi_{G_A/\rho_A},$$

откуда, ввиду (39), вытекает включение (32).

Таким образом, включение (32) равносильно соотношениям (33), (35), (37).

Обозначим через $\mathrm{Comp}_D\, H$ компоненту подгруппы H прямого произведения групп $C \times D$ в прямом множителе D.

Применяя соотношение [7]

$$\mathrm{Comp}_D\, H \simeq H/(H \cap C)$$

к подгруппе $(\mathrm{Aut}(G_A/\rho_A, G_A))_{(G_A/\rho_A)\times\Omega_A}$ группы $\Sigma(G_A/\rho_A) \times \Sigma(G_A)$, получим:

$$\begin{gathered}\mathrm{Comp}_{\Sigma(G_A)}\, (\mathrm{Aut}(G_A/\rho_A, G_A))_{(G_A/\rho_A)\times\Omega_A} \simeq \\ \simeq (\mathrm{Aut}(G_A/\rho_A, G_A))_{(G_A/\rho_A)\times\Omega_A} \Big/ (\mathrm{Aut}(G_A/\rho_A, G_A))_{(G_A/\rho_A)\times\Omega_A} \cap \Sigma(G_A/\rho_A)\end{gathered} \tag{40}$$

Из того, что включение (32) равносильно соотношениям (33), (35), (37), следует:

$$\mathrm{Comp}_{\Sigma(G_A)}\left(\mathrm{Aut}(G_A/\rho_A, G_A)\right)_{(G_A/\rho_A)\times\Omega_A} = (\Phi_A)_{\Omega_A}, \tag{41}$$

$$\begin{aligned}&(\mathrm{Aut}(G_A/\rho_A, G_A))_{(G_A/\rho_A)\times\Omega_A} \cap \Sigma(G_A/\rho_A) = \\ &= \Big((\varphi_{G_A/\rho_A}, e_{G_A}) : (a^{\rho_A})^{\varphi_{G_A/\rho_A}} = (c\cdot a)^{\rho_A}, a \in G_A,\ \rho_A^c = \rho_A,\ \exists c \in N_{G_A}(\rho_A)\Big) \simeq \\ &\simeq \Big(\varphi_{G_A/\rho_A} : (a^{\rho_A})^{\varphi_{G_A/\rho_A}} = (c\cdot a)^{\rho_A}, a \in G_A,\ \rho_A^c = \rho_A,\ \exists c \in N_{G_A}(\rho_A)\Big).\end{aligned} \tag{42}$$

Но, согласно доказательству теоремы 11.28 из [5] и замечанию после нее,

$$\begin{aligned}&\Big(\varphi_{G_A/\rho_A} : (a^{\rho_A})^{\varphi_{G_A/\rho_A}} = (c\cdot a)^{\rho_A}, a \in G_A,\ \rho_A^c = \rho_A,\ \exists c \in N_{G_A}(\rho_A)\Big) \simeq \\ &\qquad \simeq M_{G_A}^{(e)}(\rho_a)\Big/\Big(\rho_A \cap (M_{G_A}^{(E)}(\rho_A) \cap M_{G_A}^{(E)}(\rho_A))\Big).\end{aligned}$$

Теперь утверждение теоремы 2 следует из соотношений (31), (40), (41), (42).

4. Группа автоморфизмов вполне неавтономного сильно связного перестановочного автомата

Пусть G - произвольная группа, M - ее подмножество. Группу внутренних автоморфизмов группы G мы будем обозначать $\mathrm{Inn}\, G$, нормализатор M в G - через $N_G(M)$, а централизатор M в G - через $C_G(M)$.

Теорема 3. *Для произвольного вполне неавтономного сильно связного перестановочного автомата A группа $\mathrm{Aut}\, A$ является расширением группы*

$$N_{G_A}((G_A)_\alpha)\big/(G_A)_\alpha$$

при помощи группы

$$\Big((\mathrm{Aut}\, G_A)_{(G_A)_\alpha} \cdot \mathrm{Inn}\, G_A\Big)_{\Omega_A},$$

где α - произвольно выбранный и фиксированный элемент из S_A.

Доказательство. В условиях теоремы 3 полугруппа G_A является группой. Поэтому классы правой конгруэнции ρ_A на G_A - это правые смежные классы группы G_A по ее подгруппе $(G_A)_\alpha$ (см. 10.2 в [5]).

Легко видеть, что при этом:

$$M_{G_A}^{(e)}(\rho_A) = N_{G_A}((G_A)_\alpha).$$

Отсюда следует, что классы конгруэнции

$$\rho_A \cap \Big(M_{G_A}^{(e)}(\rho_A) \times M_{G_A}^{(e)}(\rho_A)\Big) = \rho_A \cap \Big(N_{G_A}((G_A)_\alpha) \times N_{G_A}((G_A)_\alpha)\Big)$$

на группе $N_{G_A}((G_A)_\alpha)$ представляют собой смежные классы этой группы по ее нормальному делителю $(G_A)_\alpha$. Таким образом:

$$M_{G_A}^{(e)}(\rho_a)\Big/\Big(\rho_A \cap \Big(M_{G_A}^{(e)}(\rho_A) \times M_{G_A}^{(e)}(\rho_A)\Big)\Big) \simeq N_{G_A}((G_A)_\alpha)\Big/(G_A)_\alpha. \quad (43)$$

Далее, классы правой конгруэнции $\rho_A^{\varphi_{G_A}}$ на G_A, где $\varphi \in \operatorname{Aut} G_A$, суть правые смежные классы группы G_A по ее подгруппе $((G_A)_\alpha)^\varphi$, а классы правой конгруэнции ρ_A^c на G_A суть правые смежные классы группы G_A по ее подгруппе $c^{-1} \cdot (G_A)_\alpha \cdot c$. Следовательно,

$$\Phi_A = \Big(\varphi \in \operatorname{Aut} G_A : \ ((G_A)_\alpha)^\varphi = c^{-1} \cdot (G_A)_\alpha \cdot c, \ \exists c \in G_A\Big).$$

Обозначим через φ_c внутренний автоморфизм группы G_A, индуцированный элементом $c \in G_A$:

$$a^{\varphi_c} = c^{-1} \cdot a \cdot c, \quad a \in G_A. \quad (44)$$

Из (44) следует, что для любого $\varphi \in \Phi_A$

$$((G_A)_\alpha)^{\varphi_c} = ((G_A)_\alpha)^\varphi$$

при некотором $c \in G_A$, откуда

$$((G_A)_\alpha)^{\varphi \cdot \varphi_c^{-1}} = (G_A)_\alpha,$$

т.е.

$$\varphi \cdot \varphi_c^{-1} \in (\Sigma(G_A))_\alpha. \quad (45)$$

Но $\varphi \cdot \varphi_c^{-1} \in \operatorname{Aut} G_A$, поэтому (45) влечет за собой:

$$\varphi \cdot \varphi_c^{-1} \in (\operatorname{Aut} G_A)_{(G_A)_\alpha},$$

откуда

$$\varphi \in (\operatorname{Aut} G_A)_{(G_A)_\alpha} \cdot \varphi_c.$$

Следовательно,

$$\Phi_A \subset (\operatorname{Aut} G_A)_{(G_A)_\alpha} \cdot \operatorname{Inn} G_A. \tag{46}$$

Пусть теперь

$$\psi \in (\operatorname{Aut} G_A)_{(G_A)_\alpha} \cdot \operatorname{Inn} G_A.$$

Тогда

$$((G_A)_\alpha)^\psi = c^{-1} \cdot (G_A)_\alpha \cdot c$$

при некотором $c \in G_A$ и, значит, $\psi \in \Phi_A$. Отсюда следует:

$$(\operatorname{Aut} G_A)_{(G_A)_\alpha} \cdot \operatorname{Inn} G_A \subset \Phi_A. \tag{47}$$

Ввиду (46) и (47),

$$(\Phi_A)_{\Omega_A} = ((\operatorname{Aut} G_A)_{(G_A)_\alpha} \cdot \operatorname{Inn} G_A)_{\Omega_A}. \tag{48}$$

Теперь утверждение теоремы 3 вытекает из теоремы 2 и соотношений (43) и (48).

Этим теорема 3 доказана.

Следствие 1. *Пусть A – вполне неавтономный сильно связный перестановочный автомат, X_A - конечное множество. Группа* $\operatorname{Aut} A$ *тогда и только тогда будет конечной, когда $(G_A)_\alpha$ имеет конечный индекс в $N_{G_A}((G_A)_\alpha)$.*

Доказательство. В условиях следствия 1

$$|((\operatorname{Aut} G_A)_{(G_A)_\alpha} \cdot \operatorname{Inn} G_A)_{\Omega_A}| \le |X_A|!$$

Поэтому группа $\operatorname{Aut} A$, согласно теореме 3, будет конечной тогда и только тогда, когда группа

$$N_{G_A}((G_A)_\alpha) \Big/ (G_A)_\alpha$$

будет конечной.

Обозначим через $\pi(G)$ множество простых делителей порядков элементов группы G, а через $\Phi(G)$ - ее подгруппу Фраттини.

Следствие 2. *Пусть A – вполне неавтономный сильно связный перестановочный автомат,*

$$|X_A| < \min_{p\in\pi(\operatorname{Aut} G_A)} p.$$

Тогда

$$\operatorname{Aut} A \simeq N_{G_A}((G_A)_\alpha)\big/(G_A)_\alpha.$$

Доказательство. Пусть $\varphi \in (\operatorname{Aut} G_A)_{\Omega_A}$, тогда ограничение $\hat{\varphi}$ преобразования φ на множество Ω_A удовлетворяет условию: $\hat{\varphi} \in \Sigma(\Omega_A)$. Поэтому, если $\hat{\varphi}$ отлично от тождественного преобразования, то любой простой делитель $\hat{p}$ порядка $\hat{\varphi}$ удовлетворяет неравенству:

$$\hat{p} \leq |\Omega_A|. \tag{49}$$

Но порядок $\hat{\varphi}$ совпадает с порядком φ, и поэтому

$$\hat{p} \in \pi(\operatorname{Aut} G_A),$$

откуда

$$\hat{p} \geq \min_{p\in\pi(\operatorname{Aut} G)} p. \tag{50}$$

Неравенство (50), по условию следствия 2, влечет за собой

$$\hat{p} \geq |X_A|. \tag{51}$$

В силу того, что A - вполне неавтономный автомат,

$$|X_A| = |\Omega_A|.$$

Следовательно, (51) противоречит неравенству (49). Отсюда вытекает, что $\hat{\varphi}$, а значит и φ - тождественное преобразование. Таким образом, $(\operatorname{Aut} G_A)_{\Omega_A} = E$.

Утверждение следствия 2 теперь получается применением теоремы 3.

Следствие 3. *Пусть A – конечный вполне неавтономный сильно связный перестановочный автомат, $|G_A| = p^n$, $|G_A : \Phi(G_A)| = p^r$, $|N_{G_A}((G_A)_\alpha) : (G_A)_\alpha| = p^d$, p - простое число. Тогда*

$$p^{r(n-r)+d} \cdot (p^r - 1) \cdot (p^r - p) \cdots (p^r - p^{r-1}) \equiv 0 \pmod{|\operatorname{Aut} A|}.$$

Доказательство. Согласно теореме Ф.Холла [8], в условиях следствия 3

$$p^{r(n-r)} \cdot (p^r - 1) \cdot (p^r - p) \cdots (p^r - p^{r-1}) \equiv 0 \pmod{|\operatorname{Aut} G_A|}.$$

Отсюда по теореме Лагранжа

$$p^{r(n-r)} \cdot (p^r - 1) \cdot (p^r - p) \cdots (p^r - p^{r-1}) \equiv 0 \pmod{|((\operatorname{Aut} G_A)_{(G_A)_\alpha} \cdot \operatorname{Inn} G_A)_{\Omega_A}|}.$$

Утверждение следствия 3 вытекает из последнего сравнения, в силу теоремы 3.

В теореме 3 описывается строение $\operatorname{Aut} A$ как абстрактной группы. Однако представляет интерес и подстановочное строение $\operatorname{Aut} A$.

В этой связи в доказываемой ниже теореме описываются компоненты $\operatorname{Aut} A$ в $\Sigma(X_A)$ и $\Sigma(S_A)$ как группы подстановок.

Предварительно введем необходимые обозначения.

Ограничение группы подстановок Φ на инвариантное относительно нее подмножество Ω ее области действия мы будем обозначать через $[\Phi]_\Omega$.

Обозначим через $G_A^{(r)}$ группу правых сдвигов правых смежных классов группы G_A по ее подгруппе $(G_A)_\alpha$, а через $G_A^{(l)}$ – группу левых сдвигов на элементы из $N_{G_A}((G_A)_\alpha)$ правых смежных классов группы G_A по ее подгруппе $(G_A)_\alpha$.

Положим:

$$\overline{(\operatorname{Aut} G_A)_{(G_A)_\alpha}} = (\overline{\varphi} \in \Sigma(\overline{S_A}),\ \varphi \in (\operatorname{Aut} G_A)_{(G_A)_\alpha} :$$
$$((G_A)_\alpha \cdot a)^{\overline{\varphi}} = (G_A)_\alpha \cdot a^{\varphi},\ a \in G_A),$$
$$\overline{\Omega}_A = (\pi_l \in \Sigma(\overline{S_A}),\ b \in \Omega_A),$$

где $\overline{S_A}$ - множество правых смежных классов группы G_A по ее подгруппе $(G_A)_\alpha$, π_b - их правый сдвиг на $b \in G_A$.

Если $H \subset \Sigma(S),\ \Omega \subset \Sigma(S)$, то $H^{(\Omega)} = H \cap N_{\Sigma(S)}(\Omega)$. $G \overset{p}{\simeq} H$ обозначает, что группы подстановок G, H подстановочно изоморфны.

Теорема 4. *Для любого вполне неавтономного сильно связного перестановочного автомата* A

$$\operatorname{Comp}_{\Sigma(X_A)} \operatorname{Aut} A \overset{p}{\simeq} \left[\left((\operatorname{Aut} G_A)_{(G_A)_\alpha} \cdot \operatorname{Inn} G_A\right)_{\Omega_A}\right]_{\Omega_A},$$

$$\operatorname{Comp}_{\Sigma(S_A)} \operatorname{Aut} A \overset{p}{\simeq} \left(\overline{(\operatorname{Aut} G_A)_{(G_A)_\alpha}} \cdot G_A^{(r)}\right)^{\overline{\Omega}_A}.$$

Доказательство. Как показано в доказательстве теоремы 2 (равносильность соотношений (19)-(20) включению (23), где φ_{X_A} и φ_{G_A} связаны посредством (21)-(22)),

$$\mathrm{Comp}_{\Sigma(X_A)}\,\mathrm{Aut}\,A = \Big[\mathrm{Comp}_{\Sigma(G_A)}(\mathrm{Aut}(S_A, G_A))_{S_A\times\Omega_A}\Big]_{\Omega_A}. \tag{52}$$

С другой стороны, согласно (41),

$$\mathrm{Comp}_{\Sigma(G_A)}(\mathrm{Aut}(S_A, G_A))_{S_A\times\Omega_A} \overset{p}{\simeq} (\Phi_A)_{\Omega_A}, \tag{53}$$

где правая часть (53) для перестановочного автомата определена в (48).

Первое соотношение теоремы 4 теперь вытекает из (52) и (53).

Для доказательства второго соотношения заметим, что согласно описанию транзитивных представлений групп подстановками [8],

$$\mathrm{Comp}_{\Sigma(S_A)}\,\mathrm{Aut}\,A \overset{p}{\simeq} \mathrm{Comp}_{\Sigma(S_{\overline{A}})}\,\mathrm{Aut}\,\overline{A}, \tag{54}$$

где $S_{\overline{A}} = \overline{S}_A$ - множество правых смежных классов G_A по $(G_A)_\alpha$, $\{X_{\overline{A}}\} = G_A$,

$$((G_A)_\alpha \cdot a)^{\delta^{(x)}_{\overline{A}}} = (G_A)_\alpha \cdot a \cdot x,\ a \in G_A,\ x \in X_{\overline{A}}.$$

Положим

$$X_{A^*} = \Omega_{A^*} = G_A,\ S_{A^*} = S_A,\ \delta^{(x)}_{A^*} = x,\ x \in X_{A^*}.$$

Ввиду равносильности соотношений (32) и (33), (35), показанной в доказательстве теоремы 2, и рассуждений в доказательстве теоремы 3,

$$\begin{aligned}&\mathrm{Comp}_{\Sigma(S_{\overline{A^*}})}\,\mathrm{Aut}\,\overline{A^*} = \Big(\psi \in \Sigma(\overline{S}_A):\\ &((G_A)_\alpha \cdot a)^\psi = (G_A)_\alpha \cdot c_{\alpha,\varphi} \cdot a^\varphi,\ a \in G_A,\ \varphi \in \Phi_A,\\ &((G_A)_\alpha)^\varphi = c^{-1}_{\alpha,\varphi} \cdot (G_A)_\alpha \cdot c_{\alpha,\varphi},\ c_{\alpha,\varphi} \in G_A\Big).\end{aligned} \tag{55}$$

Выбирая в качестве φ произвольный элемент из $(\mathrm{Aut}\,G_A)_{(G_A)_\alpha}$ и полагая $c_{\alpha,\varphi} = 1$, получим $\psi = \overline{\varphi}$.

Поэтому из (55) следует

$$\overline{(\mathrm{Aut}\,G_A)_{(G_A)_\alpha}} \subset \mathrm{Comp}_{\Sigma(\overline{S}_{A^*})}\,\mathrm{Aut}\,\overline{A^*}. \tag{56}$$

Выбирая в качестве $c_{\alpha,\varphi}$ произвольный элемент из группы G_A, а в качестве φ внутренний автоморфизм группы G_A, отвечающий этому элементу, получим, что ψ совпадает с правым сдвигом на этот элемент правых смежных классов группы G_A по ее подгруппе $(G_A)_\alpha$. Ввиду этого, из (55) следует:

$$G_A^{(r)} \subset \mathrm{Comp}_{\Sigma(\overline{S}_{A^*})} \mathrm{Aut}\, \overline{A^*}. \tag{57}$$

Включения (56) и (57) влекут за собой:

$$\overline{(\mathrm{Aut}\, G_A)_{(G_A)_\alpha}} G_A^{(r)} \subset \mathrm{Comp}_{\Sigma(\overline{S}_{A^*})} \mathrm{Aut}\, \overline{A^*}. \tag{58}$$

Пусть теперь $\psi \in \mathrm{Comp}_{\Sigma(\overline{S}_{A^*})} \mathrm{Aut}\, \overline{A^*}$, φ' - внутренний автоморфизм группы G_A, отвечающий ее элементу $c_{\alpha,\varphi}^{-1}$, $\varphi_0 = \varphi \cdot \varphi'$, где φ и $c_{\alpha,\varphi}$ соответствуют ψ как указано в (55). Тогда

$$\varphi_0 \in \overline{(\mathrm{Aut}\, G_A)_{(G_A)_\alpha}}. \tag{59}$$

Из (59) следует, что

$$\overline{\varphi}_0 \in \overline{(\mathrm{Aut}\, G_A)_{(G_A)_\alpha}}. \tag{60}$$

Для любого $a \in G_A$

$$((G_A)_\alpha \cdot a)^{\overline{\varphi}_0 \cdot \pi_{c_{\alpha,\varphi}}} = (G_A)_\alpha \cdot a^{\varphi_0} \cdot c_{\alpha,\varphi} = (G_A)_\alpha \cdot a^{\varphi \cdot \varphi'} \cdot c_{\alpha,\varphi} =$$
$$= (G_A)_\alpha \cdot c_{\alpha,\varphi} \cdot a^{\varphi} = ((G_A)_\alpha \cdot a)^{\psi},$$

откуда $\psi = \overline{\varphi}_0 \cdot \pi_{c_{\alpha,\varphi}}$. Ввиду (60), этим доказано, что

$$\mathrm{Comp}_{\Sigma(\overline{S}_{A^*})} \mathrm{Aut}\, \overline{A^*} \subset \overline{(\mathrm{Aut}\, G_A)_{(G_A)_\alpha}} G_A^{(r)}. \tag{61}$$

Сравнивая (58) и (61), заключаем:

$$\mathrm{Comp}_{\Sigma(\overline{S}_{A^*})} \mathrm{Aut}\, \overline{A^*} = \overline{(\mathrm{Aut}\, G_A)_{(G_A)_\alpha}} G_A^{(r)} \tag{62}$$

Но из начала доказательства теоремы 2 следует:

$$\mathrm{Comp}_{\Sigma(\overline{S}_A)} \mathrm{Aut}\, \overline{A} = \mathrm{Comp}_{\Sigma(\overline{S}_{A^*})} \mathrm{Aut}\, \overline{A^*},$$

так как

$$\mathrm{Comp}_{\Sigma(\overline{S}_A)} \mathrm{Aut}\, A = N_{\Sigma(S_A)}(\Omega_A).$$

Поэтому из (62) следует:

$$\mathrm{Comp}_{\Sigma(\overline{S}_A)} \mathrm{Aut}\, \overline{A} = \overline{(\mathrm{Aut}\, G_A)_{(G_A)_\alpha}} G_A^{(r)}. \tag{63}$$

Второе соотношение теоремы 4 теперь вытекает из (54) и (63).

5. Представления групп группами автоморфизмов вполне неавтономных сильно связных перестановочных автоматов

Здесь мы дадим характеризацию абстрактных групп, изоморфных группам автоморфизмов вполне неавтономных сильно связных перестановочных автоматов. При этом будем рассматривать произвольные счетные группы, и в отдельности конечно порожденные группы.

Теорема 5. *Для любой счетной группы H найдется такой вполне неавтономный сильно связный перестановочный автомат A, что* $\mathrm{Aut}\, A \simeq H$.

Доказательство. Пусть H – произвольная счетная группа, $a_1, a_2, \ldots,$ $a_n, \ldots$ - ее система образующих. Без ограничения общности будем предполагать, что $a_i \neq a_j$ при $i \neq j$. Рассмотрим группу $H_1 \simeq H$ и изоморфизм μ группы H на группу H_1.

Положим:

$$\overline{H} = H \times H_1. \tag{64}$$

Согласно (64), произвольный элемент $x \in \overline{H}$ однозначно представляется в виде:

$$x = a \cdot b^{\mu}, \quad a \in H, \quad b \in H. \tag{65}$$

Поэтому преобразование φ_0 группы $\overline{H}$, определенное выражениями (65) и

$$x^{\varphi_0} = b \cdot a^{\mu}, \tag{66}$$

является однозначным.

Это преобразование является также биективным. Действительно, если $x^{\varphi_0} = y^{\varphi_0}$, x представлено в виде (65), а $y = c \cdot d^{\mu}$, $c \in H$, $d \in H$, то, в соответствии с (66), $b \cdot a^{\mu} = d \cdot c^{\mu}$, откуда, ввиду (64), $b = d$, $a^{\mu} = c^{\mu}$, т.е. $a = c$ и, значит, $x = y$. Следовательно, φ_0 - инъективное преобразование. Сюрьективность же преобразования φ_0 вытекает из того, что, согласно (64), любой элемент $y \in \overline{H}$ можно представить в виде: $y = b \cdot a^{\mu}$, $b \in H$, $a \in H$, и потому $y = x^{\varphi_0}$, где x представлен в виде (65).

Пусть теперь $x_1 \in \overline{H}$, $x_2 \in \overline{H}$, тогда, согласно (64),

$$x_1 = a_1 \cdot b_1^{\mu}, \quad x_2 = a_2 \cdot b_2^{\mu} \tag{67}$$

для некоторых $a_1 \in H,\ b_1 \in H,\ a_2 \in H,\ b_2 \in H$.

Из (67) получаем, учитывая (66)

$$(x_1 \cdot x_2)^{\varphi_0} = (a_1 \cdot a_2 \cdot b_1^{\mu} \cdot b_2^{\mu})^{\varphi_0} = (a_1 \cdot a_2 \cdot (b_1 \cdot b_2)^{\mu})^{\varphi_0} =$$

$$= b_1 \cdot b_2 \cdot (a_1 \cdot a_2)^{\mu} = b_1 \cdot b_2 \cdot a_1^{\mu} \cdot a_2^{\mu} = (b_1 \cdot a_1^{\mu}) \cdot (b_2 \cdot a_2^{\mu}),$$

откуда, ввиду (65)-(67),

$$(x_1 \cdot x_2)^{\varphi_0} = x_1^{\varphi_0} \cdot x_2^{\varphi_0}, \quad x_1 \in \overline{H}, \quad x_2 \in \overline{H}.$$

Учитывая биективность φ_0, этим доказано, что φ_0 - автоморфизм группы $\overline{H}$. Кроме того, для любого $x \in \overline{H}$, представленого в виде (65), будем иметь:

$$x^{\varphi_0^2} = (b \cdot a^{\mu})^{\varphi_0} = a \cdot b^{\mu} = x,$$

следовательно, φ_0^2 – тождественное преобразование и, так как φ_0 не является тождественным преобразованием, то порядок φ_0 в группе $\mathrm{Aut}\,\overline{H}$ равен 2.

Поэтому существует полупрямое произведение групп:

$$G = \overline{H}\lambda\{c\}, \quad c^2 = 1, \quad c^{-1} \cdot x \cdot c = x^{\varphi_0}, \quad x \in \overline{H}. \tag{68}$$

В силу (68), группу G можно задать системой образующих:

$$\Omega = (a_1, a_1 \cdot a_2^{\mu}, \ldots, a_{n-1} \cdot a_n^{\mu}, \ldots, c). \tag{69}$$

Действительно, подгруппа группы G, порожденная множеством элементов (69), содержит элемент a_1 и, если она содержит элемент a_{n-1} при $n > 1$, то она содержит и элемент a_n^{μ}, а потому элемент $c \cdot a_n^{\mu} \cdot c^{-1} = a_n$ (см. (66-68)). Следовательно, эта подгруппа содержит H и, значит, содержит $c^{-1} \cdot H \cdot c = H^{\mu} = H_1$. Кроме того, она содержит элемент c и следовательно совпадает с G.

Теперь определим автомат A следующим образом: X_A – множество элементов (69), S_A - множество правых смежных классов группы G по подгруппе H,

$$(H \cdot a)^{\delta_A^{(x)}} = H \cdot a \cdot x, \quad a \in G, \quad x \in X_A.$$

Так как для любого $y \in H$, согласно (66) и (68),

$$c^{-1} \cdot y \cdot c \in H_1,$$

а ввиду (64) $H_1 \cap H = E$, то подгруппа H - антиинвариантная (не содержит неединичных нормальных делителей группы G). Поэтому, учитывая, что (69) - система образующих группы G, можно сделать вывод (см. [8]), что A удовлетворяет условиям теоремы 5 и

$$G_A \simeq G. \tag{70}$$

В силу теоремы 3, из (70) следует, что $\mathrm{Aut}\, A$ - расширение группы $N_G(H)/H$ при помощи группы $((\mathrm{Aut}\, G)_H \cdot \mathrm{Inn}\, G)_{X_A}$. Действительно, при изоморфизме группы G_A на группу G подгруппа $(G_A)_\alpha$ при $\alpha = H$ переходит в подгруппу H, а $\delta_A^{(x)}$ в x.

Выясним, что представляет собой группа $((\mathrm{Aut}\, G)_H \cdot \mathrm{Inn}\, G)_{X_A}$. Для этого заметим, что очевидно,

$$((\mathrm{Aut}\, G)_H \cdot \mathrm{Inn}\, G)_{X_A} \subset (\mathrm{Aut}\, G)_{X_A}. \tag{71}$$

Пусть $\varphi \in ((\mathrm{Aut}\, G)_H \cdot \mathrm{Inn}\, G)_{X_A}$.

Тогда подгруппа H^φ сопряжена с подгруппой H в группе G. Но, согласно (64), (66), (68) подгруппа H сопряжена в G только с подгруппами H и H_1.

Поэтому имеет место один из двух случаев:

$$\begin{array}{ll} I. & H^\varphi = H \\ II. & H^\varphi = H_1. \end{array}$$

Так как автоморфизм группы всегда переводит класс сопряженных подгрупп в класс сопряженных подгрупп, то, ввиду (71), φ переставляет подгруппы группы G, сопряженные с подгруппой H. Поэтому в обоих случаях $I - II$ $\overline{H}^\varphi = \overline{H}$, согласно (64). Отсюда следует, что $c^\varphi \in \overline{H}$, так как иначе $c \in \overline{H}^{\varphi^{-1}} = \overline{H}$, что противоречит (68). Но, в соответствии с выбором φ, $c^\varphi \in X_A$, поскольку $c \in X_A$. Принимая во внимание, что отличные от c элементы X_A содержатся в $\overline{H}$, включение $c^\varphi \in X_A$ при условии $c^\varphi \in \overline{H}$ влечет за собой:

$$c^\varphi = c \tag{72}$$

Будем теперь доказывать с помощью индукции, что для любого целого числа $i > 0$ имеют место равенства:

$$a_i^\varphi = a_i, \quad (a_i^\mu)^\varphi = a_i^\mu. \tag{73}$$

Начало индукции: $i = 1$. Допустим, что имеет место случай II. Тогда так как $a_1 \in H$, то $a_1^\varphi \in H_1$. Но, согласно выбору φ, $a_1^\varphi \in X_A$, поскольку $a_1 \in X_A$. Следовательно, $a_1^\varphi \in H_1 \cap X_A$. Однако этого не может быть, так как из (69) видно, что, учитывая (64) и (68), $H_1 \cap X_A = \emptyset$. Таким образом, допущение в случае II неверно, и, значит, имеет место случай I.

Следовательно, $a_1^\varphi \in H \cap X_A$. Из (69) видно, учитывая (64) и (68), что $H \cap X_A$ содержит единственный элемент, а именно a_1. Поэтому предыдущее включение влечет за собой:

$$a_1^\varphi = a_1. \tag{74}$$

В силу (65), (66), (68),

$$a_1^\mu = c^{-1} \cdot a_1 \cdot c,$$

откуда, ввиду (71), (72), (74),

$$(a_1^\mu)^\varphi = (c^\varphi)^{-1} \cdot a_1^\varphi \cdot c^\varphi = c^{-1} \cdot a_1 \cdot c = a_1^\mu. \tag{75}$$

Согласно (74) и (75), равенства (73) доказаны при $i = 1$. Сделаем теперь индуктивное предположение, что они справедливы при произвольно выбранном и фиксированном $i \geq 1$. Как видно из (69), $a_i \cdot a_{i+1}^\mu \in X_A$. Поэтому, используя (71) и (73), будем иметь:

$$(a_i \cdot a_i^\mu)^\varphi = a_i^\varphi \cdot (a_{i+1}^\mu)^\varphi = a_i \cdot (a_{i+1}^\mu)^\varphi \in X_A. \tag{76}$$

Но, согласно (69), (64), (68), X_A содержит единственный элемент из $\overline{H}$ с компонентой a_i в H, а именно $a_i \cdot a_{i+1}^\mu$, если $i > 1$ и не более двух таких элементов, а именно a_1 и $a_1 \cdot a_2^\mu$, если $i = 1$. Поэтому из (76) следует: $a_i \cdot (a_{i+1}^\mu)^\varphi = a_i \cdot a_{i+1}^\mu$, т.е. $(a_{i+1}^\mu)^\varphi = a_{i+1}^\mu$ при $i > 1$ и $a_1 \cdot (a_2^\mu)^\varphi = a_1 \cdot a_2^\mu$, откуда $(a_2^\mu)^\varphi = a_2^\mu$, либо $a_1 \cdot (a_2^\mu)^\varphi = a_1$, откуда $(a_2^\mu)^\varphi = 1$, $a_2^\mu = 1$. Следовательно,

$$(a_{i+1}^\mu)^\varphi = a_{i+1}^\mu \tag{77}$$

во всех случаях.

Но, согласно (65), (66), (68),

$$a_{i+1}^\mu = c^{-1} \cdot a_{i+1} \cdot c.$$

Поэтому, используя (71), (72), (77), будем иметь:

$$a_{i+1}^{\mu} = (c^{-1} \cdot a_{i+1} \cdot c)^{\varphi} = (c^{-1})^{\varphi} \cdot a_{i+1}^{\varphi} \cdot c^{\varphi} = c^{-1} \cdot a_{i+1}^{\varphi} \cdot c,$$

откуда

$$a_{i+1}^{\varphi} = c \cdot a_{i+1}^{\mu} \cdot c^{-1} = a_{i+1}. \tag{78}$$

Ввиду (77) и (78), индуктивный переход завершен. В силу индукции, этим равенства (73) доказаны для любого $i > 0$.

Из (72) и (73) следует, что φ действует тождественно на H, H_1, $\{c\}$ и, согласно (64) и (68), является тождественным преобразованием группы G. Ввиду произвольного выбора φ из $((\mathrm{Aut}\, G)_H \cdot \mathrm{Inn}\, G)_{X_A}$ этим доказано, что

$$((\mathrm{Aut}\, G)_H \cdot \mathrm{Inn}\, G)_{X_A} = E. \tag{79}$$

На основании (79) можно заключить, что

$$\mathrm{Aut}\, A \simeq N_G(H)/H. \tag{80}$$

Из (64) и (68) следует:

$$G \neq N_G(H) \supset \overline{H}$$

и, так как $|G : \overline{H}| = 2$, то значит

$$N_G(H) = \overline{H}.$$

Отсюда получаем, в соответствии с (64),

$$N_G(H)/H \simeq H_1. \tag{81}$$

Так как $H_1 \simeq H$, то из (80) и (81) вытекает утверждение теоремы 5.

Следствие 4. *Для любой конечно порожденной группы H, имеющей систему образующих порядка n, найдется вполне неавтономный сильно связный перестановочный автомат A, такой, что*

$$|X_A| = n + 1, \quad \mathrm{Aut}\, A \simeq H.$$

При этом, если H - конечная группа, то $\mathrm{Aut}\, A$ *- конечный автомат.*

Это следствие вытекает из того, что в условиях его для автомата A, построенного при доказательстве теоремы 5, множество X_A (69) будет иметь порядок $n + 1$, а в случае конечности H группа $G_A = G$ будет конечной.

Список литературы

[1] M.Katsura. Automorphism Groups and Factor Automata of Strongly Connected Automata. J. of Comp. and System Sci., 36, 1998

[2] A.C.Fleck. Isomorphism Groups of Automata. J. Assoc. Comput. Mach., 9, 1962.

[3] A.C.Fleck. On the Automorphism Group of an Automaton. J. Assoc. Comput. Mach., 12, 1965.

[4] Б.И.Плоткин. Группы автоморфизмов алгебраических систем. "Наука", Москва, 1966.

[5] А.Клиффорд, Г.Престон. Алгебраическая теория полугрупп. Том 2, "Мир", Москва, 1972.

[6] E.J.Tully. Representation of a semigroup by transformations acting transitively on a set. Amer. J. Math., 83.

[7] А.Г.Курош. Теория групп. "Наука", Москва, 1962.

[8] М.Холл. Теория групп. ИИЛ, Москва, 1962.