Math-Net.Ru

Общероссийский математический портал

А. В. Бабаш, М. М. Глухов, Г. П. Шанкин, О преобразованиях множества слов в конечном алфавите, не размножающих искажений, *Дискрет. матем.*, 1997, том 9, выпуск 3, 3–19

DOI: <https://doi.org/10.4213/dm481>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 34.227.88.159

26 апреля 2023 г., 07:59:06

О преобразованиях множества слов в конечном алфавите, не размножающих искажений

© 1997 г. А. В. Бабаш, М. М. Глухов, Г. П. Шанкин

Рассматриваются отображения множества слов в конечном алфавите в себя. Описаны инъективные отображения, не размножающие искажений типа замены букв в словах, биективные отображения, не размножающие искажений типа пропуска букв, и инъективные отображения, не размножающие искажений обоих указанных типов.

1. Введение

Данная работа посвящается памяти выдающегося математика Андрея Андреевича Маркова. Она инициирована одним полученным в 1956 году результатом А. А. Маркова о биективных преобразованиях φ множества слов Ω^* в конечном алфавите Ω , сохраняющих длины слов и не увеличивающих расстояния Хемминга между словами одной длины, то есть не размножающих искажений типа замены букв в словах. Рассмотренная А. А. Марковым задача имеет много различных вариаций. В частности, представляют интерес не только биективные но и инъективные отображения, наряду с искажениями типа замены букв могут происходить искажения других типов, например, пропуски букв, по разному может определяться понятие близости слов и т.д. Некоторые из таких вариаций и рассматриваются в данной работе. В параграфе 3 на основе идей А. А. Маркова описано множество $G(\Omega, \rho)$ всех инъективных отображений $\varphi: \Omega^* \rightarrow \Omega^*$, сопоставляющих словам одинаковой длины слова также одинаковой длины и не увеличивающих расстояние Хемминга ρ между словами. В качестве следствия этого описания получается и упомянутый выше результат А.А. Маркова, частный случай которого ($\Omega = \{0, 1\}$) в иной формулировке опубликован в [1], стр. 248 и [2], теорема 9. В параграфе 4 рассматривается задача описания множества $G(\Omega, \varepsilon)$ инъективных отображений $\varphi: \Omega^* \rightarrow \Omega^*$, не размножающих искажений типа пропуска букв. Однако из них полностью описаны лишь биективные преобразования. В параграфе 5 полностью описано пересечение $G(\Omega, \rho, \varepsilon)$ множеств $G(\Omega, \rho)$ и $G(\Omega, \varepsilon)$. В параграфе 6 в качестве меры близости произвольных слов (а не только слов одинаковой длины) рассматривается обобщенное расстояние Хемминга, функция ρ' , совпадающая с ρ на парах слов одинаковой длины и принимающая значение k на парах в которых одно слово получается из другого удалением k букв. Доказывается что при $|\Omega| \geq 3$ множество $G(\Omega, \rho')$ всех инъективных отображений, не увеличивающих значений функции ρ' , совпадает с пересечением множеств $G(\Omega, \rho)$ и

$G(\Omega, \varepsilon)$, хотя непосредственно из определений включение $G(\Omega, \rho')$ в каждое из этих множеств не усматривается. Заметим, что функция ρ' не является метрикой: она не удовлетворяет известному свойству треугольника.

2. Основные понятия и обозначения

В данной работе мы будем придерживаться следующих обозначений.

$\mathbf{N}$ — множество натуральных чисел;

$\mathbf{N}_0$ — множество целых неотрицательных чисел;

$[s, t] = \{s, s + 1, \dots, t\}$, где $s, t \in \mathbf{N}_0$, $s < t$;

Ω — конечный алфавит из n букв $n \geq 2$; буквы алфавита Ω и слова в алфавите Ω будут обозначаться соответственно малыми и большими латинскими буквами (с индексами и без индексов);

$P = Q$ — графическое равенство слов P и Q ;

λ — пустое слово;

$\partial(P)$ — длина слова P ;

Ω^t — множество всех слов длины $t \in \mathbf{N}_0$ в алфавите Ω , в частности, $\Omega^0 = \{\lambda\}$;

$\Omega^* = \bigcup_{t \in \mathbf{N}_0} \Omega^t$ обозначает множество всех слов в алфавите Ω ;

PQ — произведение (конкатенация) слов P, Q ;

P^t — t -я степень слова P (при любом $t \in \mathbf{N}_0$) причем $P^0 = \lambda$ для любого $P \in \Omega^*$;

$MH = \{PQ : P \in M, Q \in H\}$ — произведение множеств слов M и H ;

$P^{(i)}$ — i -я буква слова P при естественном упорядочении всех букв слова P от его начала к концу;

$P(i \rightarrow a)$ — слово, полученное из P заменой его i -й буквы на букву a ;

$P(i \rightarrow \lambda)$ — слово, полученное из P удалением его i -й буквы;

$P(i \rightarrow M) = \{P(i \rightarrow a) : a \in M\}$ для любого подмножества M из Ω ;

$P(i \downarrow a)$ — слово, полученное вставкой буквы a после i -й буквы слова P при $i \in [1, \partial(P)]$ и перед первой буквой слова P при $i = 0$;

$P(i \downarrow M) = \{P(i \downarrow a) : a \in M\}$ для любого подмножества M из Ω ;

$\rho(P, Q)$ — расстояние Хемминга между словами P, Q (одной длины); слова P и Q , для которых $\rho(P, Q) = 1$, будем называть соседними;

ε — бинарное отношение на множестве Ω^* , $P\varepsilon Q$ означает, что слово Q получено из P удалением одного вхождения некоторой его буквы;

ε^t — t -я степень бинарного отношения ε ;

$$\varepsilon(P) = \{Q \in \Omega^* : P\varepsilon Q\};$$

z — особая буква, не содержащаяся в Ω ;

$\rho'(P, Q)$ — обобщенное расстояние Хемминга между словами P и Q , определяемое как $\rho(P, Q)$ при $\partial(P) = \partial(Q)$ и как $\min \rho(P, Q_i)$ при $\partial(P) > \partial(Q)$, где минимум берется по всем словам Q_i , полученным вставками в Q ровно $\partial(P) - \partial(Q)$ вхождений особой буквы z (предполагается также, что $\rho'(P, Q) = \rho'(Q, P)$);

$\varphi(P)$ — образ слова P при отображении $\varphi: \Omega^* \rightarrow \Omega^*$;

$\varphi(M) = \{\varphi(P) : P \in M\}$ для любого подмножества слов M множества Ω^* ;

$S(M)$ — симметрическая группа подстановок множества M относительно умножения подстановок, так что для $g, h \in S(M)$ и $x \in M$

$$gh(x) = h(g(x));$$

μ — оператор обращения слов, то есть $\mu(P) = a_k a_{k-1} \dots a_1$ для слова $P = a_1 \dots a_{k-1} a_k$;

P^σ для слова $P = a_1 \dots a_{k-1} a_k$ и подстановки $\sigma \in S(\Omega)$ обозначает слово $\sigma(a_1) \dots \sigma(a_{k-1}) \sigma(a_k)$;

S_t — симметрическая группа подстановок множества $[1, t]$.

Определение 1. Отображение $\varphi: \Omega^* \rightarrow \Omega^*$ называется не размножающим искажений типа замены букв, если для любых слов $P, Q \in \Omega^*$ выполняются условия

$$\partial(P) = \partial(Q) \Rightarrow \partial(\varphi(P)) = \partial(\varphi(Q)), \quad (1)$$

$$\rho(P, Q) \geq \rho(\varphi(P), \varphi(Q)). \quad (2)$$

Определение 2. Отображение $\varphi: \Omega^* \rightarrow \Omega^*$ называется не размножающим искажений типа пропуска букв, если для любых слов $P, Q \in \Omega^*$ и любого $k \in [1, \partial(P)]$ найдется число $m \in [1, k]$ такое, что выполняется импликация

$$P\varepsilon^k Q \Rightarrow \varphi(P)\varepsilon^m \varphi(Q). \quad (3)$$

Множество всех инъективных отображений $\varphi: \Omega^* \rightarrow \Omega^*$, не размножающих искажений типа замены букв, обозначим через $G(\Omega, \rho)$, а множество всех инъективных отображений Ω^* в Ω^* , не размножающих искажений типа пропуска букв, обозначим через $G(\Omega, \varepsilon)$. Положим

$$G(\Omega, \rho, \varepsilon) = G(\Omega, \rho) \cap G(\Omega, \varepsilon).$$

Очевидно, что множества $G(\Omega, \rho)$ и $G(\Omega, \varepsilon)$ являются подполугруппами полугруппы $\Pi(\Omega^*)$ всех отображений Ω^* в Ω^* . Из них естественно выделить подгруппы биективных отображений. Обозначим их, соответственно, через $G_1(\Omega, \rho)$ и $G_1(\Omega, \varepsilon)$.

Определение 3. Отображение $\varphi: \Omega^* \rightarrow \Omega^*$ называется не увеличивающим обобщенного расстояния Хемминга между словами, если для любых $P, Q \in \Omega^*$

$$\rho'(P, Q) \geq \rho'(\varphi(P), \varphi(Q)).$$

Множество всех инъективных и биективных отображений, не увеличивающих обобщенного расстояния Хемминга между словами обозначим соответственно через $G(\Omega, \rho')$ и $G_1(\Omega, \rho')$.

3. Описание полугруппы $G(\Omega, \rho)$

Так как преобразование $\varphi \in G(\Omega, \rho)$ инъективно и удовлетворяет условию (1), при любом $t \in \mathbf{N}_0$ оно отображает множество Ω^t в $\Omega^{t+\Delta(t)}$ при некотором $\Delta(t) \in \mathbf{N}_0$. Кроме того, из инъективности φ следует, что для φ выполняется условие: для любых $t, s \in \mathbf{N}_0$, $t \neq s$,

$$t + \Delta(t) = s + \Delta(s) \Rightarrow \varphi(\Omega^t) \cap \varphi(\Omega^s) = \emptyset. \quad (4)$$

Таким образом, описание полугруппы $G(\Omega, \rho)$ сводится к описанию инъективных отображений $\varphi_t: \Omega^t \rightarrow \Omega^{t+\Delta(t)}$, $t \in \mathbf{N}_0$, удовлетворяющих условиям (2) и (4).

Опишем сначала инъективные отображения $\varphi: \Omega^t \rightarrow \Omega^{t+\Delta}$, $\Delta \in \mathbf{N}_0$, с условием (2).

Теорема 1. *Инъективное отображение $\varphi: \Omega^t \rightarrow \Omega^{t+\Delta}$ удовлетворяет условию (2) (не размножает искажений типа замены букв) тогда и только тогда, когда оно имеет вид: для любого слова $P \in \Omega^t$*

$$\varphi(P) = A_1 \sigma_1(P^{(g(1))}) A_2 \sigma_2(P^{(g(2))}) \dots A_t \sigma_t(P^{(g(t))}) A_{t+1}, \quad (5)$$

при фиксированных (не зависящих от слова P) словах $A_1, \dots, A_{t+1} \in \Omega^*$ суммарной длины $\partial(A_1 \dots A_{t+1}) = \Delta$, подстановках $\sigma_1, \dots, \sigma_t \in S(\Omega)$ и подстановке $g \in S_t$.

Доказательство. Очевидно, что любое отображение $\varphi: \Omega^t \rightarrow \Omega^{t+\Delta}$ вида (5) инъективно и обладает свойством (2). Докажем обратное утверждение. Пусть φ инъективно и удовлетворяет условию (2). Зафиксируем слово $P \in \Omega^t$ и рассмотрим множество слов $P(i \rightarrow \Omega)$, $i \in [1, t]$. Так как при $a \neq b$

$$\rho(P(i \rightarrow a), P(i \rightarrow b)) = 1,$$

в силу инъективности φ и свойства (1)

$$\rho(\varphi(P(i \rightarrow a)), \varphi(P(i \rightarrow b))) = 1$$

и поэтому

$$\varphi(P(i \rightarrow a)) = \varphi(P(\tau(i) \rightarrow h_i(a))) \quad (6)$$

при некоторых $\tau(i) \in [1, t + \Delta]$ и $h_i \in S(\Omega)$.

Ясно, что $P(i \rightarrow \Omega) \neq P(j \rightarrow \Omega)$ при $i \neq j$ и $\varphi(P(\tau(i) \rightarrow \Omega)) = \varphi(P(\tau(j) \rightarrow \Omega))$ при $\tau(i) = \tau(j)$. Отсюда и из инъективности φ получаем, что τ есть инъективное

отображение множества $[1, t]$ в $[1, t + 1]$. Таким образом, по отображению φ каждому слову $P \in \Omega^t$ сопоставлен набор подстановок $h_1, \dots, h_t \in S(\Omega)$ и инъективное отображение $\tau: [1, t] \rightarrow [1, t + 1]$, так что для всех $a \in \Omega$ и $i \in [1, t]$ выполняется равенство (6). Подставляя $a = P^{(i)}$ в (6), находим, что

$$\varphi(P)^{(\tau(i))} = h_i(P^{(i)}), \quad i \in [1, t]. \quad (7)$$

Упорядочив числа $\tau(i)$, $i \in [1, t + \Delta]$, в порядке возрастания $\tau(i_1) < \tau(i_2) < \dots < \tau(i_t)$, мы можем записать слово $\varphi(P)$ в виде

$$\varphi(P) = A_1 h_{i_1}(P^{(i_1)}) A_2 h_{i_2}(P^{(i_2)}) \dots A_t h_{i_t}(P^{(i_t)}) A_{t+1}, \quad (8)$$

где $h_j(P^{(j)})$ есть $\tau(j)$ -я буква слова $\varphi(P)$, $j \in [1, t]$, а $A_1 A_2 \dots A_{t+1}$ — слово, полученное из $\varphi(P)$ удалением букв с номерами $\tau(i_1), \dots, \tau(i_t)$. Из формулы (6) следует также, что формула (8) остается верной при замене слова P любым из слов множества $P(i \rightarrow \Omega)$ при любом $i \in [1, t]$. Подчеркнем еще, что при изменении в P буквы с номером j в слове $\varphi(P)$ изменится лишь буква с номером $\tau(j)$.

Теперь докажем, что подстановки $h_{i_1}, \dots, h_{i_t}$, отображение τ и $A_1, A_2, \dots, A_{t+1}$ не зависят от выбора слова P из Ω^t .

Так как к любому слову $Q \in \Omega^t$ можно перейти от P , меняя последовательно лишь по одной букве, указанный факт достаточно доказать лишь для соседних с P слов. Пусть $Q \in \Omega^t$, $\rho(P, Q) = 1$ и сходное с (8) представление слова Q имеет вид

$$\varphi(Q) = B_1 h'_1(Q^{(j_1)}) B_2 h'_2(Q^{(j_2)}) \dots B_t h'_t(Q^{(j_t)}) B_{t+1}, \quad (9)$$

где $h'_r(Q^{(r)})$ есть $\tau'(r)$ -я буква слова $\varphi(Q)$ и отображение $\tau': [1, t] \rightarrow [1, t + \Delta]$ определяется равенствами

$$\varphi(Q(i \rightarrow a)) = \varphi(Q(\tau'(i) \rightarrow h'_i(a))), \quad i \in [1, t], \quad a \in \Omega. \quad (10)$$

Так как $\rho(P, Q) = 1$, существует единственное число $k \in [1, t]$ такое, что $P^{(k)} \neq Q^{(k)}$. Следовательно, $P(k \rightarrow a) = Q(k \rightarrow a)$ при любом $a \in \Omega$. Отсюда и из равенств (6), (10), учитывая, что $\rho(\varphi(P), \varphi(Q)) = 1$, получаем, что $\tau'(k) = \tau(k)$ и $h'_k = h_k$ для указанного k . Далее рассмотрим слова $P(j \rightarrow a)$, $Q(j \rightarrow a)$ при $j \neq k$. Очевидно, что $\rho(P(j \rightarrow a), Q(j \rightarrow a)) = 1$, а поэтому и $\rho(\varphi(P(j \rightarrow a)), \varphi(Q(j \rightarrow a))) = 1$. Согласно формулам (8), (9) при изменении j -й буквы в словах P, Q будут меняться соответственно по подстановкам h_j , h'_j только $\tau(j)$ -я и $\tau'(j)$ -я буквы слов $\varphi(P)$, $\varphi(Q)$. Отсюда легко следует, что $\tau'(j) = \tau(j)$, $h'_j = h_j$ и $A_i = B_i$, $i \in [1, t + 1]$. Этим и доказано утверждение о независимости подстановок $h_{i_1}, \dots, h_{i_t}$, отображения τ и слов $A_1, A_2, \dots, A_{t+1}$ от выбора слова P из Ω^t . Таким образом, равенство (8) верно для всех $P \in \Omega^t$. Введя переобозначения $h_{i_s} = \sigma_s$, $i_s = g(s)$, мы получим из (8) требуемую формулу (5).

Теорема доказана.

Из всего вышесказанного в данном параграфе следует, что для построения любого отображения из $G(\Omega, \rho)$ можно выбрать произвольную последовательность $\Delta(0), \Delta(1), \dots$ чисел из $\mathbf{N}_0$ и для каждого t из $\mathbf{N}_0$ задать указанным в теореме 1 способом отображение $\varphi_t: \Omega^t \rightarrow \Omega^{t+\Delta(t)}$ так, чтобы выполнялось условие (4). Если это возможно для выбранной последовательности $\Delta(0), \Delta(1), \dots$, то последовательность $\varphi_0, \varphi_1, \dots$ определит отображение φ из $G(\Omega, \rho)$, для которого ограничение $\varphi|_{\Omega^t}$ совпадает с φ_t .

Покажем, как можно удовлетворить условие (4) при определении отображений φ_t , $t \in \mathbf{N}_0$, для заданной последовательности $\Delta(0), \Delta(1), \dots$ чисел из $\mathbf{N}_0$. Для этого заметим сначала, что номера букв слова $\varphi(P)$ из формулы (8) делятся на два класса: $M_1(\varphi)$ — множество номеров букв, изменяющихся при замене слова P другими словами из Ω^t , $M_2(\varphi)$ — множество остальных номеров (номеров неизменяющихся букв). Точнее,

$$\begin{aligned} M_1(\varphi) &= \{\tau(j) : j \in [1, t]\}, \\ M_2(\varphi) &= [1, t + \Delta(t)] \setminus M_1(\varphi). \end{aligned}$$

Из формулы (8) видно, что выбирая подходящим образом слово P , мы можем получить в качестве k -й буквы в слове $\varphi(P)$ при $k \in M_1(\varphi)$ любую букву из Ω . С другой стороны, для любого $k \in M_2(\varphi)$ буква $\varphi(P)^{(k)}$ является постоянной, не зависящей от выбора слова P (это буква слова $A_1 A_2 \dots A_{t+1}$). Следовательно, справедлива следующая теорема.

Теорема 2. *Отображение $\varphi : \Omega^* \rightarrow \Omega^*$ принадлежит $G(\Omega, \rho)$ тогда и только тогда, когда*

- (1) *ограничения $\varphi_t = \varphi \mid \Omega^t$ определены согласно теореме 1 для некоторых $\Delta(t)$, $t \in \mathbf{N}_0$;*
- (2) *для любых $t, s \in \mathbf{N}_0$, при которых $t + \Delta(t) = s + \Delta(s)$, существует такое $k \in M_2(\varphi_t) \cup M_2(\varphi_s)$, что*

$$\varphi_t(P)^{(k)} \neq \varphi_s(Q)^{(k)},$$

где $P \in \Omega^t$, $Q \in \Omega^s$.

Отметим, что условие 2 данной теоремы вполне конструктивно.

В частном случае, когда все числа $\Delta(t)$ равны нулю, получается следующая теорема А. А. Маркова.

Теорема 3. *Биективное отображение $\varphi : \Omega^* \rightarrow \Omega^*$ не размножает искажений типа замены букв в словах тогда и только тогда, когда для любого слова $P \in \Omega^t$, $t \in \mathbf{N}$, оно задается формулой*

$$\varphi(P) = \sigma_{t1}(P^{(g_t(1))}) \dots \sigma_{tt}(P^{(g_t(t))}),$$

где $\{\sigma_{ij} : i \in \mathbf{N}, j \in [1, i]\}$ — любой набор подстановок из $S(\Omega)$, а $g_1, g_2, \dots$ — любой набор подстановок, соответственно, из $S_1, S_2, \dots$.

4. Описание группы $G_1(\Omega, \varepsilon)$

Напомним, что $G_1(\Omega, \varepsilon)$ есть множество всех биективных отображений $\varphi : \Omega^* \rightarrow \Omega^*$, удовлетворяющих условию (3). Докажем сначала несколько общих утверждений о преобразованиях из полугруппы $G(\Omega, \varepsilon)$.

Предложение 1. *Для любого $\varphi \in G(\Omega, \varepsilon)$, любых слов $P, Q \in \Omega^*$ и числа $k \in \mathbf{N}$ справедлива импликация*

$$P \varepsilon^k Q \Rightarrow \varphi(P) \varepsilon^k \varphi(Q). \quad (11)$$

Доказательство. Согласно определению степени ε^k бинарного отношения ε , соотношение $P\varepsilon^k Q$ означает существование последовательности $P = P_1, P_2, \dots, P_{k+1} = Q$ такой, что $P_1\varepsilon P_2\varepsilon \dots \varepsilon P_{k+1}$. Отсюда и из условия (3), учитывая инъективность отображения φ , получаем, что

$$\varphi(P_1)\varepsilon\varphi(P_2)\varepsilon \dots \varepsilon\varphi(P_{k+1}),$$

что означает $\varphi(P)\varepsilon^k\varphi(Q)$.

Предложение 2. Для любого $\varphi \in G(\Omega, \varepsilon)$ существует $\Delta = \Delta(\varphi) \in \mathbf{N}_0$ такое, что при каждом $t \in \mathbf{N}_0$

$$\varphi(\Omega^t \subseteq \Omega^{t+\Delta}.$$

Доказательство. Пусть $\varphi \in G(\Omega, \varepsilon)$, $\varphi(\lambda) = P$ и $\partial(P) = \Delta$. Тогда для любого слова $A \in \Omega^t$ при $t \geq 1$ имеем $A\varepsilon^t\lambda$ и в силу (11) получаем, что $\varphi(A)\varepsilon^t P$. Отсюда видно, что $\partial(\varphi(A)) = t + \partial(P) = \partial(A) + \Delta$. Следовательно, $\varphi(\Omega^t) \subseteq \Omega^{t+\Delta}$.

Предложение 3. Отображение φ из $G(\Omega, \varepsilon)$ биективно тогда и только тогда, когда оно сохраняет длины слов.

Доказательство. Если $\varphi \in G(\Omega, \varepsilon)$ сохраняет длины слов, то биективность φ следует из его инъективности. Если же оно биективно, то указанное в предложении 2 число $\Delta(\varphi)$ равно нулю, а это и означает, что φ сохраняет длины слов.

Предложение 4. Множество $G_1(\Omega, \varepsilon)$ всех биективных отображений из $G(\Omega, \varepsilon)$ является группой.

Доказательство. Замкнутость множества $G_1(\Omega, \varepsilon)$ относительно операции умножения отображений очевидна. Поэтому достаточно показать, что

$$\varphi \in G_1(\Omega, \varepsilon) \Rightarrow \varphi^{-1} \in G_1(\Omega, \varepsilon),$$

то есть

$$P\varepsilon Q \Rightarrow \varphi^{-1}(P)\varepsilon\varphi^{-1}(Q)$$

для любых $P, Q \in \Omega^*$. Из условия сохранения длин слов (предложение 3) отображением φ следует, что для слов P, Q найдется натуральное число m такое, что $\varphi^m(P) = P$, $\varphi^m(Q) = Q$. Тогда $\varphi^{-1}(P) = \varphi^{m-1}(P)$, $\varphi^{-1}(Q) = \varphi^{m-1}(Q)$, и доказываемая импликация является следствием замкнутости множества $G_1(\Omega, \varepsilon)$ относительно произведения отображений.

Из предложений 1 и 4 следует, что любое отображение $\varphi \in G_1(\Omega, \varepsilon)$ перестановочно с отношением ε , то есть для любого $P \in \Omega^*$

$$\varphi(\varepsilon(P)) = \varepsilon(\varphi(P)). \quad (12)$$

В дальнейшем нам понадобятся еще некоторые чисто технические утверждения о словах из Ω^* .

Лемма 1. Если $P \in \Omega^t$, $a, b \in \Omega$ и $aP = Pb$, то $a = b$ и $P = a^t$.

Для доказательства леммы 1 достаточно провести побуквенное сравнение слов aP и Pb .

Лемма 2. Если $P \in \Omega^t$, $a, b \in \Omega$ и

$$\rho(aP, Pb) = 1, \quad (13)$$

то $a \neq b$ и $P = a^k b^m$ при некоторых $k, m \in \mathbb{N}_0$.

Доказательство. Из условия (13) следует существование единственного значения $i \in [1, t+1]$, при котором $(aP)^{(i)} \neq (Pb)^{(i)}$. Пусть $(aP)^{(i)} = c$, $(Pb)^{(i)} = d$. Тогда при $i > 1$ слово P имеет вид $P_1 c d P_2$ и из (13) получаем, что

$$aP_1 = P_1 c, \quad dP_2 = P_2 b.$$

Отсюда и из леммы 1 следует утверждение леммы 2.

Лемма 3. Любое слово P длины $\partial(P) \geq 3$ однозначно определяется множеством слов $\varepsilon(P)$.

Доказательство. Для слова P возможны три варианта:

$$\begin{aligned} P &= a^t; \\ P &= a^k b P_1; \\ P &= a b P_2, \end{aligned}$$

где $a, b \in \Omega$, $a \neq b$, $P_1, P_2 \in \Omega^*$, $P_2 \neq \lambda$, $t \geq 3$, $k \geq 2$. Они характеризуются следующими свойствами множества $\varepsilon(P)$:

- в первом случае $\varepsilon(P)$ состоит из одного слова a^{t-1} ;
- во втором случае все слова из $\varepsilon(P)$ начинаются с буквы a , причем одно из них есть $a^{k-1} b P_1$, все другие имеют начало a^m , $m \geq k$;
- в третьем случае $\varepsilon(P)$ содержит слова $a P_2$, $b P_2$, а все остальные слова, если они есть, имеют начало ab , при этом таких слов может не быть лишь в том случае, когда $P_2 = b^r$.

Очевидно, что по указанной информации легко не только различить эти три варианта, но и однозначно найти слово P .

Из леммы 3, в частности, следует, что для любых слов $P, Q \in \Omega^*$ длины $t \geq 3$ выполняется импликация

$$\varepsilon(P) = \varepsilon(Q) \Rightarrow P = Q. \quad (14)$$

Лемма 4. Если для некоторых слов $P_1, P_2, Q \in \Omega^*$ и различных букв $a, b \in \Omega$ выполняются соотношения

$$P_1 a P_2 \varepsilon Q, \quad P_1 b P_2 \varepsilon Q,$$

то $Q = P_1 P_2$.

Доказательство. По условию слово Q получено удалением по одной букве из слов P_1aP_2 , P_1bP_2 . Если удалялось выделенное вхождение буквы a из слова P_1aP_2 или буквы b из P_1bP_2 , то утверждение верно. Кроме того, поскольку $a \neq b$, слово Q не могло получиться удалением из слов P_1aP_2 , P_1bP_2 по одной букве из P_1 или по одной букве из P_2 . Следовательно, возможна лишь ситуация, где

$$P_1 = P'_1cP''_1, \quad P_2 = P'_2dP''_2$$

и либо

$$Q = P'_1P''_1aP_2 = P_1bP'_2P''_2,$$

либо

$$Q = P'_1P''_1bP_2 = P_1aP'_2P''_2.$$

В силу симметрии достаточно рассмотреть один из указанных случаев. Пусть имеет место первый случай, то есть

$$Q = P'_1P''_1aP'_2dP''_2 = P'_1cP''_1bP'_2P''_2.$$

Тогда $P''_1aP'_2d = cP''_1bP'_2$, в частности, $P''_1a = cP''_1$, $P'_1d = bP'_2$. Отсюда по лемме 1 получаем, что $a = c$, $P''_1 = a^k$, $d = b$, $P'_2 = d^m$. Следовательно,

$$\begin{aligned} Q &= P'_1a^ka^mdP''_2 = P'_1aa^kdd^mP''_2, \\ P_1 &= P'_1aa^k, \quad P_2 = d^mP'_2, \end{aligned}$$

откуда получаем, что $Q = P_1P_2$ и лемма доказана.

Теперь можно перейти к формулировке и доказательству основного результата данного параграфа.

Теорема 4. *Отображение $\varphi: \Omega^* \rightarrow \Omega^*$ содержится в группе $G_1(\Omega, \varepsilon)$ тогда и только тогда, когда $\varphi(P)$ для любого $P \in \Omega^*$ имеет вид*

$$\varphi(P) = P^\sigma \tag{15}$$

или

$$\varphi(P) = \mu(P^\sigma), \tag{16}$$

где σ — фиксированная для данного φ подстановка из $S(\Omega)$, а μ — оператор обращения слов.

Доказательство. Очевидно, что отображения вида (15), (16) содержатся в $G_1(\Omega, \varepsilon)$. Докажем обратное утверждение. Пусть $\Omega = \{a_1, \dots, a_n\}$ и $\varphi \in G_1(\Omega, \varepsilon)$. Так как φ биективно, оно по предложению 3 сохраняет длины слов, в частности, $\varphi(\lambda) = \lambda$ и $\varphi(a_i) = \sigma(a_i)$, $i \in [1, n]$, для некоторой подстановки $\sigma \in S(\Omega)$. Покажем, что при этой подстановке σ отображение φ действует, как в (15) или как в (16), на всех словах P длины 2.

Для $n \leq 2$ этот факт следует непосредственно из (12), биективности φ и сохранения им длин слов.

Пусть $n \geq 3$. Обозначим для краткости $\sigma(a_i) = b_i$, $i \in [1, n]$. Так как $\varepsilon(a_i a_j) = \{a_i, a_j\}$ при $i \neq j$, в силу (12)

$$\varepsilon(\varphi(a_i a_j)) = \{\varphi(a_i), \varphi(a_j)\} = \{b_i, b_j\}.$$

Отсюда, учитывая биективность φ , находим, что

$$\varphi(a_i a_j) = b_i b_j, \quad \varphi(a_j a_i) = b_j b_i \quad (17)$$

или

$$\varphi(a_i a_j) = b_j b_i, \quad \varphi(a_j a_i) = b_i b_j. \quad (18)$$

Докажем, что при выполнении условия (17) для некоторых фиксированных различных $i, j \in [1, n]$ необходимо выполняются равенства

$$\varphi(a_i a_k) = b_i b_k \quad (19)$$

при любом $k \neq i$. Допустим, что при некотором $k \neq i$, $k \neq j$ справедливо равенство $\varphi(a_i a_k) = b_k b_i$ и, значит, $\varphi(a_k a_i) = b_i b_k$. Рассмотрим слово $Q = a_i a_j a_k$. Так как $\varepsilon(Q) = \{a_i a_j, a_i a_k, a_j a_k\}$, в силу (12)

$$\varepsilon(\varphi(Q)) = \{b_i b_j, b_k b_i, \varphi(a_j a_k)\}.$$

Отсюда однозначно находим, что

$$\varphi(Q) = b_k b_i b_j, \quad \varphi(a_j a_k) = b_k b_j, \quad \varphi(a_k a_j) = b_j b_k.$$

Теперь для слова $Q_1 = a_i a_k a_j$

$$\varepsilon(Q_1) = \{a_i a_k, a_i a_j, a_k a_j\}$$

и в силу (12) получаем, что

$$\varepsilon(\varphi(Q_1)) = \{b_k b_i, b_i b_j, b_j b_k\}.$$

Однако нетрудно видеть, что слова Q_1 , удовлетворяющего последнему условию, не существует (так как ни одна из букв b_i, b_j, b_k не может быть первой буквой в слове $\varphi(Q_1)$). Значит, наше допущение невозможно, то есть верно (19). Из доказанного легко следует, что если равенства (17) выполняются для некоторых фиксированных различных i, j , то они выполняются для произвольных различных $i, j \in [1, n]$. Из соображений симметрии то же самое верно и относительно условия (18). Заметим еще, что теперь равенства

$$\varphi(a_i a_i) = b_i b_i, \quad i \in [1, n],$$

следуют непосредственно из условия (12). Таким образом, φ действует по правилу (15) или по правилу (16) на всех словах длины $L \leq 2$.

Допустим, что последнее утверждение верно для всех слов длины $L \leq t$ и докажем его для всех слов длины $t + 1$.

Пусть $\varphi(P) = P^\sigma$ для всех $P \in \Omega^t$, а Q — любое слово длины $t + 1$. Тогда, используя (13) и очевидное равенство $(\varepsilon(Q))^\sigma = \varepsilon(Q^\sigma)$ получим, что

$$\varepsilon(\varphi(Q)) = \varphi(\varepsilon(Q)) = (\varepsilon(Q))^\sigma = \varepsilon(Q^\sigma).$$

Отсюда, в силу (14), $\varphi(Q) = Q^\sigma$.

Если же $\varphi(P) = \mu(P^\sigma)$ для всех $P \in \Omega^t$, то аналогично, используя перестановочность преобразования μ с отношением ε и преобразованием $P \rightarrow P^\sigma$, получим, что

$$\varphi(Q) = \mu(Q^\sigma)$$

для любого слова $Q \in \Omega^{t+1}$. Теорема доказана.

Непосредственно из теорем 1, 3 получается следующее утверждение.

Следствие 1. *Справедливо включение*

$$G_1(\Omega, \varepsilon) \subset G_1(\Omega, \rho).$$

5. Описание полугруппы $G(\Omega, \rho, \varepsilon)$

Теорема 5. *Инъективное отображение $\varphi: \Omega^* \rightarrow \Omega^*$ содержится в полугруппе $G(\Omega, \rho, \varepsilon)$ тогда и только тогда, когда для любого $P \in \Omega^*$ отображение $\varphi(P)$ имеет вид*

$$\varphi(P) = AP^\sigma B \quad (20)$$

или

$$\varphi(P) = A\mu(P^\sigma)B \quad (21)$$

при фиксированных для заданного φ словах $A, B \in \Omega^*$ и подстановке $\sigma \in S(\Omega)$.

Доказательство. Непосредственно из теорем 1–4 видно, что отображения вида (20) и (21) содержатся в полугруппе $G(\Omega, \rho, \varepsilon) = G(\Omega, \rho) \cap G(\Omega, \varepsilon)$. Докажем обратное утверждение. По предложению 2 для любого $\varphi \in G(\Omega, \varepsilon)$ существует число $\Delta \in \mathbb{N}$ такое, что для любого $t \in \mathbb{N}$ справедливо включение $\varphi(\Omega^t) \subseteq \Omega^{t+\Delta}$. Если $\Delta = 0$, то φ биективно, и по теореме 3 имеет требуемый вид (20) или (21) при $A = B\lambda$.

Пусть $\Delta \geq 1$. Согласно теореме 1 (при $t = 1$) $\varphi(a_i) = A\sigma(a_i)B$ для любой буквы a_i из Ω , где A, B — фиксированные слова, σ — фиксированная подстановка из $S(\Omega)$. Так как $a_i \varepsilon \lambda$, то $\varphi(a_i) \varepsilon \varphi(\lambda)$, $i \in [1, n]$. Отсюда, учитывая, что $|\Omega| = n \geq 2$ по лемме 4 получаем, что $\varphi(\lambda) = AB$. Таким образом, доказываемое относительно φ утверждение верно для всех слов P длины $L \leq 1$. Для общего индуктивного перехода нам понадобится еще доказать его и для слов длины 2, поскольку на словах длины $L \leq 1$ преобразования φ , определяемые формулами (20) и (21), действуют одинаково. По теореме 1 (при $t = 2$) образ $\varphi(P)$ любого слова P длины 2 находится по формуле

$$\varphi(P) = A_1\sigma_1(P^{(g(1))})A_2\sigma_2(P^{(g(2))})A_3$$

при некоторых $A_1, A_2, A_3 \in \Omega^*$, $\sigma_1, \sigma_2 \in S(\Omega)$, $g \in S_2$. В зависимости от подстановки g возможны два случая:

$$\varphi(P) = A_1\sigma_1(P^{(1)})A_2\sigma_2(P^{(2)})A_3;$$

$$\varphi(P) = A_1\sigma_1(P^{(2)})A_2\sigma_2(P^{(2)})A_3.$$

В первом случае

$$\begin{aligned}\varphi(P(1 \rightarrow a)) &= A_1 \sigma_1(a) A_2 \sigma_2(P^{(2)}) A_3, \\ \varphi(P(2 \rightarrow a)) &= A_1 \sigma_1(P^{(1)}) A_2 \sigma_2(a) A_3.\end{aligned}$$

Так как $P(i \rightarrow a) \varepsilon P(i \rightarrow \lambda)$, то $\varphi(P(i \rightarrow a)) \varepsilon \varphi(P(i \rightarrow \lambda))$. Отсюда, учитывая, что $n \geq 2$, по лемме 4 получаем, что

$$\varphi(P(1 \rightarrow \lambda)) = A_1 A_2 \sigma_2(P^{(2)}) A_3, \quad \varphi(P(2 \rightarrow \lambda)) = A_1 \sigma_1(P^{(1)}) A_2 A_3. \quad (22)$$

С другой стороны по доказанному для $t = 1$

$$\varphi(P(1 \rightarrow \lambda)) = A \sigma(P^{(2)}) B, \quad \varphi(P(2 \rightarrow \lambda)) = A \sigma(P^{(1)}) B. \quad (23)$$

Приравнивая правые части соответствующих равенств из (22) и (23), получим, что $A_1 = A$, $A_2 = \lambda$, $A_3 = B$, $\sigma_1 = \sigma_2 = \sigma$, и значит,

$$\varphi(P) = A P^\sigma B.$$

Аналогично во втором случае получим, что

$$\varphi(P) = A \mu(P^\sigma) B.$$

Далее в индуктивном переходе необходимо рассмотреть два случая, когда для всех слов длины $t < L$, где $L \geq 3$, действие отображения φ задается соответственно формулами (20), (21). В обоих этих случаях при рассмотрении слов длины L повторяются те же рассуждения, что и выше при $t = 2$. А именно, сравниваются значения слова $\varphi(P(i \rightarrow \lambda))$, найденные по лемме 4 с использованием формулы (5) и по предположению индукции (при всех возможных $P \in \Omega^t$, $i \in [1, t]$). В обоих случаях получим, что

$$A_1 = A, \quad A_2 = A_3 = \dots = A_t = \lambda, \quad A_{t+1} = B, \quad \sigma_1 = \sigma_2 = \dots = \sigma_t = \sigma,$$

а подстановка g в первом случае будет тождественной, а во втором она равна

$$\begin{pmatrix} 1 & 2 & \dots & t-1 & t \\ t & t-1 & \dots & 2 & 1 \end{pmatrix}.$$

Отсюда следует, что утверждение теоремы справедливо для всех слов длины $L \leq t$, $t \geq 3$. Теорема доказана.

6. Описание полугруппы $G(\Omega, \rho')$

Заметим, что хотя значение ρ' на парах слов одной длины совпадает со значением ρ , включение $G(\Omega, \rho') \subseteq G(\Omega, \rho)$ непосредственно из определений 1, 3 не следует, поскольку при определении множества $G(\Omega, \rho)$ на отображения $\varphi: \Omega^* \rightarrow \Omega^*$ налагалось дополнительное требование (1). Кроме того, непосредственно из определений $G(\Omega, \rho')$ и $G(\Omega, \varepsilon)$ не следует также, что $G(\Omega, \rho') \subseteq G(\Omega, \varepsilon)$. Дело в том, что из $P \varepsilon Q$ следует, что $\rho'(P, Q) = 1$, однако обратная импликация неверна. Вместе с тем, имеет место следующее утверждение.

Теорема 6. Если $|\Omega| = n \geq 3$, то

$$G(\Omega, \rho') = G(\Omega, \rho) \cap G(\Omega, \varepsilon). \quad (24)$$

В случае $\Omega = 2$ вопрос о справедливости равенства (24) остается открытым.

Для доказательства теоремы 6 введем некоторые дополнительные понятия и обозначения.

Пусть P — фиксированное слово из Ω^* . Множество слов $M \subset \Omega^*$ назовем P -системой, а слова из M назовем P -совместимыми, если для любых $A, B \in M$

$$\rho'(A, B) = \rho'(P, A) = 1.$$

P -систему назовем максимальной, если она не входит ни в какую отличную от нее P -систему.

Опишем максимальные P -системы. Для $P = \lambda$ единственной такой системой является Ω . Пусть $P \in \Omega^t$, $t \geq 1$. В этом случае множество

$$O(P) = \{Q \in \Omega^*: \rho'(P, Q) = 1\},$$

содержащее все P -системы, представляется в виде объединения

$$O(P) = \varepsilon(P) \cup \left(\bigcup_{i=0}^t P(i \downarrow \Omega) \cup \left(\bigcup_{i=1}^t P(i \rightarrow \Omega) \setminus P^{(i)} \right) \right).$$

Выясним вопрос о совместимости слов из различных компонент этого объединения.

Лемма 5. Пусть A, B — два различных P -совместимых слова для слова $P \neq \lambda$. Тогда

- (1) $A \in \varepsilon(P) \Rightarrow B \notin P(i \downarrow \Omega)$, $i \in [0, t]$;
- (2) $A \in \varepsilon(P)$, $B \in P(i \rightarrow \Omega) \Rightarrow P = P_1 a P_2$, $A = P_1 P_2$, $B = P_1 b P_2$ при некоторых $P_1, P_2 \in \Omega^*$, $a, b \in \Omega$, $a \neq b$;
- (3) $A, B \in \varepsilon(P) \Rightarrow P = P_1 a b P_2$, $A = P_1 a P_2$, $B = P_1 b P_2$ при некоторых $P_1, P_2 \in \Omega^*$, $a, b \in \Omega$, $a \neq b$;
- (4) если некоторое слово C совместимо с A, B и $A, B, C \in \varepsilon(P)$, то $C = A$ или $C = B$;
- (5) $A \in P(i \downarrow \Omega)$, $B \in P(j \rightarrow \Omega) \Rightarrow P = P_1 b P_2$, $A = P_1 a b P_2$, $B = P_1 a P_2$ или $A = P_1 b a P_2$, $B = P_1 a P_2$, $a \neq b$;
- (6) если $A \in P(i \downarrow \Omega)$, $B \in P(j \downarrow \Omega)$, то существует $r \in [0, t]$, при котором $A, B \in P(r \downarrow \Omega)$;
- (7) $A \in P(i \rightarrow \Omega) \Rightarrow B \notin P(j \rightarrow \Omega)$ для $j \neq i$.

Доказательство. 1. Если $A \in \varepsilon(P)$, $B \in P(i \downarrow \Omega)$, то $\partial(B) - \partial(A) = 2$. Поэтому $\rho'(A, B) \geq 2$ и A, B не могут быть P -совместимыми.

2. Пусть $A = P(j \rightarrow \lambda)$, $B \in P(i \rightarrow b)$. Если $i = j$, то утверждение верно. Пусть $i < j$. Тогда

$$P = R_1 a R_2 c R_3, \quad A = R_1 a R_2 R_3, \quad B = R_1 b R_2 c R_3, \quad a \neq b.$$

Так как $\partial(A) = \partial(B) - 1$, при нахождении $\rho'(A, B)$ в слово A должна вставляться особая буква z так, чтобы для полученного слова A' выполнялось условие $\rho(A', B) = 1$. Так как $a \neq b$, буква z может быть вставлена только в R_1 . Значит, $A = R'_1 z''_1 a R_2 R_3$ и из условия $\rho(A', B) = 1$ получаем, что

$$\rho(z R''_1, R''_1 b) = 1, \quad \rho(a R_2, R_2 c) = 0.$$

Отсюда, используя леммы 1 и 2, находим, что $a = c$, $R_2 = a^k$, $R = b^m$. Подставляя найденные результаты в P , A и B , замечаем, что утверждение 2 выполняется при $P_1 = R_1$, $P_2 = R_2 c R_3$. Справедливость утверждения 2 при $i > j$ устанавливается аналогично.

3. Пусть $A = P(i \rightarrow \lambda)$, $B = P(j \rightarrow \lambda)$. Так как $A \neq B$, то $i \neq j$. Пусть $i < j$. Тогда

$$P = R_1 a R_2 b R_3, \quad A = R_1 R_2 b R_3, \quad B = R_1 a R_2 R_3.$$

Так как $\partial(A) = \partial(B)$, то $\rho'(A, B) = \rho(A, B)$ и из условия $\rho(A, B) = 1$ получаем, что $\rho(R_2 b a R_2) = 1$. Отсюда по лемме 2 находим, что $a \neq b$, $R_2 = a^k b^m$. Следовательно, утверждение 3 выполняется при $P_1 = R_1 a^k$, $P_2 = b^m R_3$.

4. Допустим, что A, B, C попарно различны. В силу симметричности условий для слов A, B, C , не теряя общности, можно считать, что

$$P = R_1 a R_2 b R_3 c R_4, \quad A = R_1 R_2 b R_3 c R_4, \quad B = R_1 a R_2 R_3 c R_4, \quad C = R_1 a R_2 b R_3 R_4.$$

Применяя утверждение 3 к парам слов (A, B) , (B, C) , (A, C) , получим равенства

$$R_2 = a^k b^m, \quad R_3 = b^r c^s, \quad R_2 b R_3 = a^p c^q.$$

Отсюда видно, что $b = a$ или $b = c$. В первом случае $A = B$, во втором $B = C$. Получили противоречие.

5. Это утверждение доказывается так же, как утверждение 2, с рассмотрением двух подслучаев $i < j$ и $i \geq j$.

6. Пусть $A = P(i \downarrow a)$, $B \in P(j \downarrow b)$ и $i < j$. Тогда

$$P = R_1 R_2 R_3, \quad A = R_1 a R_2 R_3, \quad B = R_1 R_2 b R_3.$$

Отсюда и из условия $\rho(A, B) = 1$ по лемме 2 получаем, что $R_2 = a^k b^m$, $a \neq b$, и утверждение 6 выполняется при $P_1 = R_1 a^k$, $P_2 = b^m R_3$.

7. Если $A \in P(i \rightarrow \Omega)$, $B \in P(j \rightarrow \Omega)$, то очевидно, что при $i \neq j$ справедливы равенства $\rho'(A, B) = \rho(A, B) = 2$, и получаем противоречие. Лемма доказана.

Лемма 6. Если $P \in \Omega^t$, $|\Omega| = n \geq 3$ и $t \geq 1$, то максимальные по мощности P -системы слов исчерпываются множествами вида

- (a) $P(i \downarrow \Omega)$, $i \in [0, t]$;
- (b) $P(i \rightarrow (\Omega \setminus \{P^{(i)}\}) \cup \{P(i \rightarrow \lambda)\})$, $i \in [1, t]$;

Доказательство. Используем утверждения 1–7 леммы 5. Очевидно, что P -системы типа (a) и (b) содержат по n элементов. Покажем, что любая другая P -система слов содержит менее n элементов. Пусть $P \in \Omega^t$, $t \geq 1$ и M — максимальная

по мощности P -система. По утверждению 4 леммы 5 M содержит не более двух различных слов из $P(\varepsilon)$. В связи с этим возможны три случая.

1. $A, B \in M \cap \varepsilon(P)$, $A \neq B$. Тогда согласно утверждению 3

$$P = P_1 ab P_2, \quad A = P_1 a P_2, \quad B = P_1 b P_2, \quad a \neq b.$$

Кроме того, согласно утверждению 1 $M \cap P(i \downarrow \Omega) = \emptyset$, $i \in [0, t]$, а в силу утверждения 7 может существовать лишь единственное значение i , при котором $M \cap P(i \rightarrow \Omega) \neq \emptyset$. Пусть $C \in M \cap P(i \downarrow \Omega)$. Тогда в силу утверждения 2

$$C = P_1 ac P_2 = P_1 db P_2, \quad c \neq b, \quad d \neq a.$$

Получили противоречие. Значит, в этом случае $M = 2 < n$.

2. $M \cap \varepsilon(P) = \{A\}$. Здесь, как и выше, из утверждений 1 и 7 получим, что M может содержать слова лишь из $P(i \rightarrow \Omega)$ при некотором одном значении $i \in [1, t]$. В последнем случае, согласно утверждению 2, $P = P_1 a P_2$, и M состоит из слов $P_1 P_2$, $P_1 b P_2$, $b \neq a$, то есть M — P -система типа (b).

3. $M \cap \varepsilon(P) = \emptyset$. Здесь согласно утверждению 7 возможны два подслучая.

3.1. $P(i \rightarrow \Omega) \cap M = \emptyset$ для всех $i \in [1, t]$. Тогда в силу утверждения 6 $M \in P(j \downarrow \Omega)$ для некоторого $j \in [0, t]$ и значит, M есть P -система типа (a).

3.2. Существует единственное значение i , при котором $P(i \rightarrow \Omega) \cap M \neq \emptyset$. Если $M \subseteq P(i \rightarrow \Omega)$, то $|M| < n$. В противном случае согласно утверждению 6 существует единственное значение $j \in [0, t]$ такое, что $M \cap P(j \downarrow \Omega) \neq \emptyset$. Тогда согласно утверждению 5 справедливо представление $P = P_1 b P_2$ и M может содержать лишь слова вида $P_1 a P_2$, $P_1 ab P_2$ или $P_1 a P_2$, $P_1 ba P_2$, $a \neq b$. Так как при различных a, b, c

$$\rho'(P_1 ab P_2, P_1 c P_2) = 2,$$

M не может содержать более двух слов и поэтому $|M| < n$. Лемма доказана.

Доказательство теоремы 6. Из теоремы 5 следует, что $G(\Omega, \rho) \cap G(\Omega, \varepsilon) \subseteq G(\Omega, \rho')$. Докажем обратное включение. Пусть $\varphi \in G(\Omega, \rho')$. Так как φ инъективно и не увеличивает значений функции ρ' , то φ любую P -систему слов переводит в $\varphi(P)$ -систему для любого $P \in \Omega^*$. В частности, максимальные P -системы типов (a) и (b) переводятся отображением φ в $\varphi(P)$ -системы типов (a) и (b).

Докажем что P -система типа (a) может отображаться лишь в $\varphi(P)$ -систему типа (a) для любого слова $P \in \Omega^*$.

Допустим, что для некоторого слова P некоторая его P -система M типа (a) отображается в $\varphi(P)$ -систему типа (b). Тогда

$$P = P_1 P_2, \quad M = \{P_1 a_i P_2 : i \in [1, n]\}, \quad \varphi(P) = Q_1 a_m Q_2, \\ \varphi(M) = \{Q_1 Q_2\} \cup \{Q_1 a_i Q_2 : i \in [1, n], i \neq m\}$$

и для некоторого фиксированного $h \in [1, n]$

$$\varphi(P_1 a_h P_2) = Q_1 Q_2, \quad \varphi(P_1 a_i P_2) = Q_1 b_i Q_2, \quad i \in [1, n], \quad i \neq h.$$

Заметим, что в последнем равенстве при изменении a_i буква b_i принимает все значения из $\Omega \setminus \{a_m\}$. Рассмотрим еще $P_1 a_r P_2$ -систему типа (a)

$$M' = \{P_1 a_r a_i P_2 : i \in [1, n]\}$$

при фиксированном $r \in [1, n]$, $r \neq h$. Для нее возможны два случая.

В первом случае $\varphi(M')$ есть $\varphi(P_1 a_r P_2)$ -система типа (а). Тогда

$$Q_2 = Q'_2 Q''_2, \quad \varphi(P_1 a_r a_i P_2) = Q_1 b_r Q'_2 c_i Q''_2, \quad i \in [1, n]$$

или

$$Q_1 = Q'_1 Q''_1, \quad \varphi(P_1 a_r a_i P_2) = Q'_1 c_i Q''_1 b_r Q_2, \quad i \in [1, n].$$

В обоих вариантах имеем противоречие с определением φ , поскольку

$$\rho'(P_1 a_h P_2, P_1 a_r a_h P_2) = 1, \quad \rho'(\varphi(P_1 a_h P_2), \varphi(P_1 a_r a_h P_2)) = 2.$$

Во втором случае $\varphi(M')$ есть $\varphi(P_1 a_r P_2)$ -система типа (b). Тогда в силу симметрии можно считать что $Q_1 = Q'_1 c Q''_1$ и при некотором фиксированном $s \in [1, n]$

$$\varphi(P_1 a_r a_s P_2) = Q'_1 Q''_1 b_r Q_2, \quad \varphi(P_1 a_r a_j P_2) = Q'_1 c_j Q''_1 b_r Q_2, \quad j \in [1, n], \quad j \neq s, \quad c_j \neq c.$$

Докажем, что $h = s$. Допустим, что это не так. Тогда из условия

$$\rho'(P_1 a_r a_h P_2, P_1 a_h P_2) = 1$$

получаем, что

$$\rho'(Q'_1 c_h Q''_1 b_r Q_2, Q'_1 c Q''_1 Q_2) = 1.$$

Отсюда точно так же, как в доказательстве утверждения 2 леммы 5, из условия $\rho'(A, B) = 1$ получим, что $b_r = c$ и $Q''_1 = c^k$ при некотором $k \in \mathbb{N}_0$. Используя эти равенства, приходим к соотношениям

$$(P_1 a_r a_s P_2) = Q'_1 c^k c Q_2, \quad \varphi(P_1 a_h P_2) = Q'_1 c c^k Q_2,$$

противоречащим инъективности φ . Таким образом, $h = s \neq r$ и в силу условия $n \geq 3$ найдется $j \in [1, n]$, $j \neq h, s, r$. Тогда

$$\begin{aligned} \rho'(P_1 a_i P_2, P_1 a_r a_i P_2) &= 1, \\ \rho'(\varphi(P_1 a_j P_2), \varphi(P_1 a_r a_j P_2)) &= \rho'(Q'_1 c Q''_1 b_j Q_2, Q'_1 c_i Q''_1 b_r Q_2) = 2, \end{aligned}$$

что противоречит определению φ .

Итак, во всех логически возможных случаях наше допущение ведет к противоречию. Значит φ переводит P -системы типа (а) в $\varphi(P)$ -системы типа (а) и P -системы типа (b) в $\varphi(P)$ -системы типа (b) для любого слова $P \in \Omega^*$.

Теперь, используя этот факт, покажем, что $\varphi \in G(\Omega, \varepsilon)$. Пусть для некоторых слов $P, Q \in \Omega^*$ выполнено соотношение $P \varepsilon Q$, то есть P, Q имеют вид

$$P = P_1 a P_2, \quad Q = P_1 P_2$$

при некоторых $P_1, P_2 \in \Omega^*$, $a \in \Omega$. Рассмотрим P -систему типа (b)

$$M = \{P_1 P_2\} \cup \{P_1 a_i P_2 : a_i \neq a\}.$$

По доказанному φ переводит ее в $\varphi(P)$ -систему типа (b). Это означает, что

$$\varphi(P) = R = R_1 b R_2, \quad \varphi(M) = \{R_1 R_2\} \cup \{R_1 b_j R_2 : b_j \neq b\}.$$

Если при этом $\varphi(P_1 P_2) \neq R_1 R_2$, то

$$\varphi(P_1 P_2) = R_1 b_s R_2, \quad \varphi(P_1 a_r P_2) = R_1 R_2$$

при некоторых $b_s \neq b$, $a_r \neq a$. Отсюда, учитывая, что $\varphi(P_1 a P_2) = R_1 b R_2$, получаем, что φ переводит $P_1 P_2$ -систему $\{P_1 a_i P_2 : a_i \in \Omega\}$ типа (а) в $\varphi(P_1 P_2)$ -систему типа (b). Полученное противоречие доказывает, что $\varphi(P_1 P_2) = R_1 R_2$, то есть $\varphi(Q) = R_1 R_2$. Следовательно, верно соотношение $\varphi(P)\varepsilon\varphi(Q)$ и потому $\varphi \in G(\Omega, \varepsilon)$. Отсюда и из предложения 2 следует, в частности, что φ удовлетворяет условию (2). А так как на словах одной длины функция ρ' совпадает с ρ , то $\varphi \in G(\Omega, \rho)$. Таким образом, $\varphi \in G(\Omega, \rho) \cap G(\Omega, \varepsilon)$, и теорема доказана.

Замечание 1. В практических приложениях представляет интерес рассмотрение биективных отображений конечного множества $\Omega^0 \cup \Omega \dots \cup \Omega^L$ в себя, не распространяющих искажений. Из доказательств приведенных утверждений легко видеть, что и в этом случае вид таких отображений остается таким же.

Список литературы

1. Гаврилов Г. П., Сапоженко А. А. *Задачи и упражнения по курсу дискретной математики*. Наука, Москва, 1992.
2. Носов В. А. *Основы комбинаторной теории*. Москва, 1990.

Статья поступила 23.10.1996.