Math-Net.Ru

Общероссийский математический портал

И. И. Резников, В. И. Сущанский, Автоматы Мили промежуточного роста с двумя состояниями над двухбуквенным алфавитом, *Матем. заметки*, 2002, том 72, выпуск 1, 102–117

DOI: <https://doi.org/10.4213/mzm408>

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: 54.92.164.108

26 апреля 2023 г., 15:15:28

УДК 519.713

АВТОМАТЫ МИЛИ ПРОМЕЖУТОЧНОГО РОСТА С ДВУМЯ СОСТОЯНИЯМИ НАД ДВУХБУКВЕННЫМ АЛФАВИТОМ

И. И. Резников, В. И. Сущанский

Изучаются автоматы с двумя состояниями над двухбуквенными алфавитами, имеющие промежуточный рост. Анализируется асимптотическое поведение функции роста. Найдена система определяющих соотношений и доказано, что их число не может быть конечным.

Библиография: 25 названий.

1. Введение. Понятие роста является одним из основных в современной комбинаторной алгебре [1], [2]. В теорию групп оно вошло после работ А. С. Шварца [3] и, особенно, Дж. Милнора [4]. Исследования же роста полугрупп было начато несколько позже. Основной проблемой касательно роста алгебраических объектов является определение возможных функций роста и исследование их связей с различными свойствами объектов. В 1968 году Милнор [5] и Вольф [6] установили, что каждая конечнопорожденная разрешимая группа имеет или полиномиальный, или экспоненциальный рост. В своей замечательной теореме М. Громов [7] дал описание групп полиномиального роста: каждая такая группа является конечным расширением нильпотентной группы. В 1988 году Р. И. Григорчук [8] получил аналогичный результат для конечнопорожденных полугрупп с сокращениями.

Большим стимулом в исследованиях по указанной тематике явилась поставленная Дж. Милнором проблема о существовании групп промежуточного роста. Эта проблема была решена в 1984 году Григорчуком [9], [10]. Первые примеры полугрупп промежуточного роста были построены несколько раньше (см., например, [11]). Полугруппы промежуточного роста могут обладать дополнительными свойствами, не имеющими аналогов в теории групп. Так, например, промежуточный рост могут иметь линейные полугруппы над полями [12], [13], относительно свободные полугруппы некоторых многообразий [14]; в [15] Григорчук указал связи между ростом и аменабельностью полугрупп.

Конструкции групп промежуточного роста, первоначально предложенные Р. И. Григорчуком, а затем и другими авторами (см. [16], а также [17]), могут быть описаны на нескольких эквивалентных языках: автоморфизмов корневых деревьев, изометрий неархимедовых метрик, преобразований, определяемых автоматами Мили. В этой связи дальнейшее развитие получили исследования по теории автоматных преобразований, целью которых было построение автоматов Мили, определяющих новые группы и полугруппы промежуточного роста (см. обзор [17] и список литературы в нем). В результате

автоматы промежуточного роста с t состояниями над n -элементным алфавитом были построены при $t \geq 2$, $n \geq 3$ либо $t \geq 3$, $n \geq 2$ [16], [18]. Вопрос о существовании автоматов с двумя состояниями над двухэлементным алфавитом, имеющих промежуточный рост, оставался открытым. В данной работе мы строим такие автоматы и устанавливаем, что полугруппа, ими определяемая, имеет промежуточный рост.

Ранее нами было проведено исследование функций роста всех 256 автоматов с двумя состояниями над двухэлементным алфавитом [19], [20] (множество всех таких автоматов будем обозначать $\mathcal{A}_{2 \times 2}$). Для этой цели был разработан программный комплекс, с помощью которого были получены таблицы значений функций роста автоматов из $\mathcal{A}_{2 \times 2}$ при небольших значениях аргумента (не более 100).

На множестве всех таких автоматов естественным образом определяется отношение эквивалентности: эквивалентными считаются автоматы, получаемые друг из друга перестановками состояний или букв алфавита. Эквивалентные автоматы порождают одинаковые полугруппы преобразований и функции роста. Множество всех автоматов с двумя состояниями над двухбуквенным алфавитом разбивается на 76 классов эквивалентности. При этом (см. [19]–[21]) автоматы из 48 классов эквивалентности порождают конечные полугруппы, автоматы из 10 классов эквивалентности порождают полугруппы линейного роста, а автоматы из 17 классов эквивалентности порождают полугруппы экспоненциального роста.

Отсюда следует, что имеется не более одного класса эквивалентности (состоящего в точности из четырех автоматов), автоматы которого имеют промежуточный рост.

Пусть f_1, f_2 – преобразования над множеством $\{a, b\}^*$, задаваемые автоматом A в состояниях q_1 и q_2 соответственно, S_A – полугруппа, порождаемая этими преобразованиями.

Основными результатами работы являются следующие утверждения.

ТЕОРЕМА 1. *Полугруппа S_A является моноидом и имеет следующее задание образующими и определяющими соотношениями:*

$$S_A = \langle f_1, f_2 \mid f_1^2 = \text{Id}; f_2(f_1 f_2)^k (f_2 f_1)^k f_2^2 = f_2(f_1 f_2)^k (f_2 f_1)^k, k \geq 0 \rangle, \quad (1)$$

причем проблема равенства слов в полугруппе S_A разрешима за линейное время.

Задание (1) полугруппы S_A дает возможность вычислить ее функцию роста в явном виде. Пусть $R_{p,m}$ – количество разбиений натурального числа p на m ненулевых слагаемых, R_p – количество всех разбиений числа p на слагаемые.

ТЕОРЕМА 2. *Функция роста $\gamma_S(n)$ полугруппы S_A определяется равенством*

$$\gamma_S(n) = (2n + 1) + 2 \sum_{l=1}^{n-2} \sum_{m=1}^{\lfloor \sqrt{l} \rfloor} \sum_{p=m}^{d(l,m)} R_{p,m} + \sum_{m=1}^{\lfloor \sqrt{n-1} \rfloor} \sum_{p=m}^{d(n-1,m)} R_{p,m}, \quad (2)$$

где $d(l, m) = \lfloor \frac{1}{2}((l+1) - (m-1)^2) \rfloor$.

Из теоремы 2, учитывая асимптотическую формулу Харди–Рамануджана для $R_{p,m}$ (см. [22], а также [23, с. 271]), получаем

СЛЕДСТВИЕ. Для любого $\varepsilon > 0$ при достаточно больших n выполняется неравенство

$$(2n+1) + \frac{1-\varepsilon}{2\pi\sqrt{2}}\sqrt{n-2}e^{\pi\sqrt{2/3}\sqrt[4]{n-2}}\left(\frac{4\sqrt{6}}{\pi} + (n-2)^{-3/4}\right) < \gamma_S(n) < (2n+1) + \frac{1+\varepsilon}{2\pi}e^{\pi\sqrt{n}/\sqrt{3}}\left(\frac{4\sqrt{3}}{\pi} + n^{-1/2}\right). \quad (3)$$

В частности, функция $\gamma_S(n)$ имеет промежуточный характер роста, причем

$$[e^{\sqrt[4]{n}}] \leq [\gamma_S] \leq [e^{\sqrt{n}}]. \quad (4)$$

2. Вспомогательные сведения. Пусть $T = (X, Q, \pi, \lambda)$ – конечный автомат Мили, входной и выходной алфавиты которого совпадают и равны, $X = \{x_1, x_2, \dots, x_n\}$, $Q = \{q_1, q_2, \dots, q_m\}$ – его множество внутренних состояний, $\pi: X \times Q \rightarrow Q$ и $\lambda: X \times Q \rightarrow X$ – функции переходов и выходов соответственно. Если требуется уточнить, какой автомат участвует в построениях, будем указывать его нижним индексом.

Каждому состоянию $q \in Q$ автомата T поставим в соответствие преобразование $\sigma_{q,T}$ над алфавитом X , которое задается функцией выходов λ :

$$\sigma_{q,T} = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ \lambda(x_1, q) & \lambda(x_2, q) & \dots & \lambda(x_n, q) \end{pmatrix}.$$

Пусть X^* – множество всех слов в алфавите X . Функции π и λ стандартным образом расширяются до отображений множества $X^* \times Q$ во множества Q и X^* соответственно, а именно:

$$\begin{aligned} \pi(\Lambda, q) &= q, & \pi(wx, q) &= \pi(x, \pi(w, q)), \\ \lambda(\Lambda, q) &= \Lambda, & \lambda(wx, q) &= \lambda(w, q)\lambda(x, \pi(w, q)), \end{aligned}$$

где $\Lambda \in X^*$ – пустое слово, $q \in Q$, $w \in X^*$, $x \in X$.

Преобразование $f_{q,T}(u) = \lambda(u, q)$, $u \in X^*$, называется *автоматным преобразованием*, определяемым автоматом T в состоянии $q \in Q$. Автомат T с множеством состояний $Q = \{q_1, q_2, \dots, q_m\}$ определяет совокупность преобразований $\{f_{q_1,T}, f_{q_2,T}, \dots, f_{q_m,T}\}$.

Автоматы T_1 и T_2 называются *эквивалентными*, если они определяют одно и то же множество преобразований над множеством X^* . В классе эквивалентных между собой (конечных) автоматов существует с точностью до изоморфизма единственный *минимальный* (по числу состояний) автомат Мили, который строится стандартным образом с помощью алгоритма минимизации (см., например, [24]).

По определению для каждого состояния $q \in Q$ действие автоматного преобразования $f_{q,T}$ на входное слово $u = u_1 u_2 \dots u_n$ можно записать следующим образом:

$$\begin{aligned} f_{q,T}(u) &= f_{q,T}(u_1 u_2 \dots u_n) = \lambda(u_1, q) f_{\pi(u_1, q), T}(u_2 \dots u_n) \\ &= \sigma_{q,T}(u_1) f_{\pi(u_1, q), T}(u_2 \dots u_n), \end{aligned}$$

т.е. автоматное преобразование $f_{q,T}$ на первую букву слова действует преобразованием алфавита $\sigma_{q,T}$, а на остаток слова без первой буквы – преобразованием $f_{\pi(u_1,T),T}$. Поэтому преобразования, определяемые автоматом T , можно записывать в *развернутом виде*, а именно:

$$f_{q_i} = (f_{\pi(x_1,q_i)}, f_{\pi(x_2,q_i)}, \dots, f_{\pi(x_n,q_i)}) \sigma_{q_i},$$

где $i = 1, 2, \dots, m$.

Произведением автоматов $T_1 = (X, Q_1, \pi_1, \lambda_1)$ и $T_2 = (X, Q_2, \pi_2, \lambda_2)$ называется автомат $T = (X, Q_1 \times Q_2, \pi, \lambda)$, функции π и λ которого определены равенствами

$$\begin{aligned} \pi(x, (q_1, q_2)) &= (\pi_1(x, q_1), \pi_2(\lambda(x, q_1), q_2)), \\ \lambda(x, (q_1, q_2)) &= \lambda_2(\lambda_1(x, q_1), q_2), \end{aligned}$$

где $x \in X$, $(q_1, q_2) \in Q_1 \times Q_2$. Заметим, что при умножении автоматы записываются слева направо, а произведения автоматных преобразований, ими определяемые, – справа налево.

Для любого автомата T определена его степень T^n при произвольном натуральном n . В общем случае T^n не является минимальным автоматом, и результат применения алгоритма минимизации к T^n обозначим $T^{(n)}$. Из определения произведения автоматов следует, что $|Q_{T^{(n)}}| \leq |Q_T|^n$.

ЛЕММА 1 [25]. *Для любых состояний $q_1 \in Q_1$, $q_2 \in Q_2$ автоматов T_1, T_2 и произвольного слова $u \in X^*$ выполнено равенство*

$$f_{(q_1, q_2), T_1 \times T_2}(u) = f_{q_2, T_2}(f_{q_1, T_1}(u)).$$

Из леммы 1 следует, что для преобразований f_{q_1, T_1} и f_{q_2, T_2} , $q_1 \in Q_1$ и $q_2 \in Q_2$, развернутая форма их произведения $f_{(q_1, q_2), T_1 \times T_2}$ определяется равенством

$$\begin{aligned} f_{(q_1, q_2), T_1 \times T_2} &= f_{q_2, T_2} f_{q_1, T_1} \\ &= (f_{\pi(\sigma_{q_1, T_1}(x_1), q_2), T_2} f_{\pi(x_1, q_1), T_1}, \dots, f_{\pi(\sigma_{q_1, T_1}(x_n), q_2), T_2} f_{\pi(x_n, q_1), T_1}) \sigma_{q_2, T_2} \sigma_{q_1, T_1}. \end{aligned} \quad (5)$$

Функцией роста автомата Мили T называется [8] функция $\gamma_T(n)$ натурального аргумента, которая определяется равенством

$$\gamma_T(n) = |Q_{T^{(n)}}|, \quad n \in \mathbb{N}.$$

Полугруппой преобразований, порожденной автоматом Мили T с множеством состояний $Q = \{q_1, q_2, \dots, q_m\}$, называется полугруппа $S_T = \langle f_{q_1, T}, f_{q_2, T}, \dots, f_{q_m, T} \rangle$. Для обратимых автоматов Мили, т.е. таких, что функция выходов $\lambda(x, q)$ при любом $q \in Q$ определяет перестановку над множеством X , рассматривается *группа преобразований*, порожденная автоматом.

Функцией роста полугруппы (группы) S относительно системы порождающих P называется функция $\gamma_S(n)$ натурального аргумента n , равная количеству элементов S , представимых в виде произведения длины не более n элементов из P .

Монотонно неубывающие функции натурального аргумента γ_1 и γ_2 имеют *одинаковый порядок роста* или *эквивалентны*, если существуют натуральные числа $C_1, C_2, N_0 \in \mathbb{N}$ такие, что для всех $n \geq N_0$ одновременно выполняются неравенства $\gamma_1(n) \leq \gamma_2(C_1 n)$ и $\gamma_2(n) \leq \gamma_1(C_2 n)$. Эквивалентность функций будем обозначать символом $\sim$, а классы эквивалентности функций называть *порядками роста*.

Связь между ростом автомата и ростом полугруппы преобразований, им порожденной, дается следующим утверждением.

ЛЕММА 2 [8]. 1. Для произвольного автомата T при любом $n \in \mathbb{N}$ значение $\gamma_T(n)$ совпадает с числом элементов полугруппы S_T , представимых в виде произведения длины n образующих $\{f_{q_1, T}, f_{q_2, T}, \dots, f_{q_m, T}\}$.

2. Для любого автомата T имеет место соотношение

$$\gamma_T \sim \gamma_{S_T}.$$

3. Доказательство теоремы 1. Для доказательства теоремы 1 потребуется несколько лемм, в которых устанавливаются свойства полугруппы S_A . Обозначим $\mathfrak{S}_2$ полугруппу преобразований над алфавитом $\{a, b\}$, т.е.

$$\mathfrak{S}_2 = \left\{ e = \begin{pmatrix} a & b \\ a & b \end{pmatrix}, \sigma = \begin{pmatrix} a & b \\ b & a \end{pmatrix}, \sigma_a = \begin{pmatrix} a & b \\ a & a \end{pmatrix}, \sigma_b = \begin{pmatrix} a & b \\ b & b \end{pmatrix} \right\}.$$

По определению $\sigma_{q_1, A}, \sigma_{q_2, A} \in \mathfrak{S}_2$. Запишем преобразования f_1 и f_2 , определяемые автоматом A , в развернутом виде

$$f_1 = (f_1, f_1)\sigma, \quad f_2 = (f_2, f_1)\sigma_b. \quad (6)$$

Согласно (6) преобразование f_1 действует на входное слово $u = u_1 u_2 \dots u_n$ таким образом:

$$f_1(u) = f_1(u_1 u_2 \dots u_n) = \sigma(u_1) f_1(u_2 \dots u_n) = \dots = \sigma(u_1) \sigma(u_2) \dots \sigma(u_n).$$

Отсюда сразу же получаем следующую лемму.

ЛЕММА 3. Преобразование f_1 является инволюцией.

Таким образом, полугруппа S_A является моноидом, и, как обычно, полагаем, что нулевая степень ее элементов равна тождественному преобразованию. Из (5) и (6) следует, что для любого натурального числа $k \geq 1$ выполняются равенства

$$(f_2 f_1)^k = ((f_2 f_1)^{k-1}, (f_2 f_1)^k) \sigma_b \quad \text{и} \quad (f_1 f_2)^k = ((f_1 f_2)^k, (f_1 f_2)^{k-1}) \sigma_a. \quad (7)$$

Построим теперь бесконечную серию соотношений между образующими f_1 и f_2 полугруппы S_A .

ЛЕММА 4. Для любого натурального числа $k \geq 0$ имеют место равенства

$$r_k : f_2 (f_1 f_2)^k (f_2 f_1)^k f_2^2 = f_2 (f_1 f_2)^k (f_2 f_1)^k. \quad (8)$$

ДОКАЗАТЕЛЬСТВО проведем индукцией по числу k .

Пусть $k = 0$. Покажем, что преобразование $f_2(f_1f_2)^0(f_2f_1)^0f_2^2 = f_2^3$ совпадает с преобразованием $f_2(f_1f_2)^0(f_2f_1)^0 = f_2$. Используя лемму 3, имеем

$$f_2^3 = (f_2, f_1)\sigma_b \cdot (f_2, f_1)\sigma_b \cdot (f_2, f_1)\sigma_b = (f_1^2f_2, f_1^3)\sigma_b = (f_2, f_1)\sigma_b = f_2.$$

Пусть $k > 0$. Из (7) для преобразования $f_2(f_1f_2)^k(f_2f_1)^k$ получаем

$$\begin{aligned} f_2(f_1f_2)^k(f_2f_1)^k &= (f_2, f_1)\sigma_b \cdot ((f_1f_2)^k, (f_1f_2)^{k-1})\sigma_a \cdot ((f_2f_1)^{k-1}, (f_2f_1)^k)\sigma_b \\ &= (f_2(f_1f_2)^{k-1}(f_2f_1)^{k-1}, f_2(f_1f_2)^{k-1}(f_2f_1)^k)\sigma_b, \end{aligned} \quad (9)$$

а для преобразования $f_2(f_1f_2)^k(f_2f_1)^kf_2^2$, учитывая (9), имеем

$$\begin{aligned} f_2(f_1f_2)^k(f_2f_1)^kf_2^2 &= (f_2(f_1f_2)^{k-1}(f_2f_1)^{k-1}, f_2(f_1f_2)^{k-1}(f_2f_1)^k)\sigma_b \cdot (f_1f_2, \text{Id})\sigma_b \\ &= (f_2(f_1f_2)^{k-1}(f_2f_1)^kf_1f_2, f_2(f_1f_2)^{k-1}(f_2f_1)^k)\sigma_b \\ &= (f_2(f_1f_2)^{k-1}(f_2f_1)^{k-1}f_2^2, f_2(f_1f_2)^{k-1}(f_2f_1)^k)\sigma_b. \end{aligned} \quad (10)$$

По предположению индукции правые части (9) и (10) совпадают, т.е. соотношение r_k выполняется.

Перепишем систему соотношений (8) в следующем виде:

$$\begin{aligned} r_0 : f_2^3 &= f_2, \\ r_k : f_2(f_1f_2)^kf_2(f_1f_2)^kf_2 &= f_2(f_1f_2)^kf_2(f_1f_2)^{k-1}f_1, \quad k \geq 1. \end{aligned}$$

Левую часть определяющего соотношения r_k , $k \geq 1$, обозначим v_k , т.е.

$$v_k = f_2(f_1f_2)^kf_2(f_1f_2)^kf_2.$$

ЛЕММА 5. *Бесконечная система соотношений*

$$f_1^2 = \text{Id} \quad \text{и} \quad r_0, r_1, r_2, \dots \quad (11)$$

является независимой, т.е. ни одно из ее соотношений не выводится из других.

ДОКАЗАТЕЛЬСТВО. Рассмотрим полугрупповое слово f_1^2 . Поскольку каждое соотношение r_k в обеих частях содержит символ f_2 , то к слову f_1^2 нельзя применить ни одно из соотношений r_k , $k \geq 0$. Отсюда следует, что соотношение $f_1^2 = \text{Id}$ не выводится из системы соотношений r_k , $k \geq 0$.

Покажем, что никакое соотношение r_k не является следствием остальных соотношений системы (11). Рассмотрим слово v_k . Оно преобразуется в слово меньшей длины только с помощью соотношения r_k , но никакого другого соотношения из (11). В самом деле, длину слова v_k нельзя уменьшить с помощью соотношения $f_1^2 = \text{Id}$, так как v_k не содержит подслов f_1^2 . Распирение слова v_k вставкой подслов f_1^2 не позволяет применить другие соотношения из (11) и не приводит к сокращению слова v_k .

Слово v_k нельзя сократить с помощью соотношений r_m , $m \neq k$, так как оно не содержит подслов v_m при $m \neq k$, т.е. применить соотношение r_m нельзя. С другой стороны, слово v_k содержит правые части соотношений r_m для $m < k$, но в этом случае получаем

$$\begin{aligned} v_k &= f_2(f_1 f_2)^k f_2(f_1 f_2)^k f_2 = f_2(f_1 f_2)^{k-m} \underbrace{(f_1 f_2)^m f_2(f_1 f_2)^{m-1} f_1 f_2(f_1 f_2)^{k-m} f_2}_{r_m} \\ &= f_2(f_1 f_2)^{k-m} (f_1 f_2)^m f_2(f_1 f_2)^{m-1} f_1 f_2^2 f_2(f_1 f_2)^{k-m} f_2 \\ &= f_2(f_1 f_2)^k f_2(f_1 f_2)^k f_2 = v_k, \end{aligned}$$

т.е. применение соотношения r_m ничего не дает. Таким образом, соотношение r_k нельзя вывести из остальных соотношений системы (11).

Отметим, что применение любого определяющего соотношения к некоторому полугрупповому слову изменяет длину этого слова на четное количество символов.

ЛЕММА 6. *С помощью соотношений системы (11) любой элемент полугруппы S_A может быть преобразован к следующему виду:*

$$s = f_1^{\varepsilon_1} f_2(f_1 f_2)^{p_1} f_2(f_1 f_2)^{p_2} f_2 \dots (f_1 f_2)^{p_m} f_2(f_1 f_2)^{p_{m+1}} f_1^{\varepsilon_2}, \quad (12)$$

где $0 \leq \varepsilon_1 \leq \varepsilon_2 \leq 1$, $0 \leq \varepsilon_1 + \varepsilon_2 \leq 1$ при $m = -1$ и $\varepsilon_1, \varepsilon_2 \in \{0, 1\}$, $0 \leq p_1 < p_2 < p_3 < \dots < p_m$, $p_{m+1} \geq 0$ при $m \geq 0$; причем алгоритм приведения состоит не более чем из $\lfloor |s|/2 \rfloor$ шагов.

ДОКАЗАТЕЛЬСТВО. Пусть s – произвольный элемент длины l полугруппы S_A . Так как S_A порождается двумя образующими $\{f_1, f_2\}$, то s имеет следующий вид:

$$s = f_1^{p_1} f_2^{p_2} f_1^{p_3} f_2^{p_4} \dots f_1^{p_{k-1}} f_2^{p_k}, \quad (13)$$

где $k \geq 1$, $p_1, p_k \geq 0$, $p_i \geq 1$, $1 < i < k$, $\sum_{1 \leq i \leq k} p_i = l$.

Применение определяющих соотношений $f_1^2 = \text{Id}$ и r_0 полугруппы S_A позволяет уменьшить показатели p_i в (13), а именно: образующая f_1 может встречаться в степени не выше первой, а образующая f_2 – в степени не выше второй. Если после такого сокращения элемент s равен единице или f_1 , то запишем его в виде (12), положив $m = -1$:

$$\begin{aligned} s = \text{Id} &= f_1^0 f_1^0, & \varepsilon_1 = 0, & \varepsilon_2 = 0, & m = -1; \\ s = f_1 &= f_1^0 f_1^1, & \varepsilon_1 = 0, & \varepsilon_2 = 1, & m = -1. \end{aligned}$$

В противном случае сгруппируем вместе подслова вида $f_1 f_2$ и (13) перепишем в виде, подобном (12):

$$s = f_1^{\varepsilon_1} f_2(f_1 f_2)^{p_1} f_2(f_1 f_2)^{p_2} f_2 \dots (f_1 f_2)^{p_m} f_2(f_1 f_2)^{p_{m+1}} f_1^{\varepsilon_2}, \quad (14)$$

где $m \geq 0$, $\varepsilon_1, \varepsilon_2 \in \{0, 1\}$, $p_i \geq 1$, $i = 1, 2, \dots, m+1$.

Если в (14) входит подслово v_k для некоторого индекса $k \geq 1$, то s можно сократить и получить элемент $s' \in S_A$ меньшей длины. Поэтому полугрупповое слово s будет

несократимым тогда и только тогда, когда оно не содержит подслов v_k для всех $k \geq 1$. Предположим, что в слове s существует подслово

$$w_{p,q} = f_2(f_1 f_2)^p f_2(f_1 f_2)^q f_2, \quad (15)$$

где $p \geq q$. Так как слово $w_{p,q}$ можно представить в виде

$$w_{p,q} = (f_2 f_1)^{p-q} f_2(f_1 f_2)^q f_2(f_1 f_2)^q f_2 = (f_2 f_1)^{p-q} v_q,$$

то в этом случае s можно сократить с помощью соотношения r_q . Окончательно, полугрупповое слово s вида (14) с помощью определяющих соотношений (11) нельзя преобразовать к слову меньшей длины тогда и только тогда, когда оно не содержит подслов вида (15) для $p \geq q \geq 0$ или, что тоже самое, когда выполняется условие

$$p_i < p_{i+1}, \quad i = 1, 2, \dots, m-1, \quad (16)$$

откуда приходим к требуемому виду (12) несократимых слов полугруппы S_A .

Для приведения элемента s , записанного в виде (13), к виду (12) можно воспользоваться следующим алгоритмом:

- 1) слово s сокращается применением определяющего соотношения $f_1^2 = \text{Id}$;
- 2) слово s сокращается применением определяющего соотношения r_0 ;
- 3) после шагов 1 и 2 слово записывается в виде (14);
- 4) если для показателей p_i вида (14) выполнено условие (16), то алгоритм закончен, так как s имеет вид (12), в противном случае переходим к следующему шагу;
- 5) для первой пары показателей p_j и p_{j+1} , $1 \leq j \leq m-1$, таких, что $p_j \geq p_{j+1}$, применяем соотношение r_{j+1} , которое сокращает слово s на подслово f_2^2 длины 2;
- 6) переходим на шаг 1.

Понятно, что результат применения данного алгоритма для произвольного элемента s – приведение его к виду (12). Так как на каждом шаге данного алгоритма применяется одно из определяющих соотношений системы (11), что уменьшает длину полугруппового слова на два символа, то алгоритм заканчивает работу не более чем за $\lceil |s|/2 \rceil$ шагов.

Заметим, что эту оценку нельзя улучшить. Любой элемент вида (12) требует 0 шагов для приведения, а элемент f_1^l – в точности $\lceil l/2 \rceil$ шагов.

Назовем вид (12) *приведенным* и в дальнейшем элементы будем записывать в приведенном виде.

ЛЕММА 7. *Элементы s_1 и s_2 вида*

$$\begin{aligned} s_1 &= f_1^{\varepsilon_1} f_2(f_1 f_2)^{p_1} f_2(f_1 f_2)^{p_2} f_2 \dots (f_1 f_2)^{p_m} f_2(f_1 f_2)^{p_{m+1}} f_1^{\varepsilon_2}, \\ s_2 &= f_1^{\mu_1} f_2(f_1 f_2)^{q_1} f_2(f_1 f_2)^{q_2} f_2 \dots (f_1 f_2)^{q_l} f_2(f_1 f_2)^{q_{l+1}} f_1^{\mu_2}, \end{aligned}$$

где $m, l \geq 0$, $\varepsilon_1, \varepsilon_2 \in \{0, 1\}$, $\mu_1, \mu_2 \in \{0, 1\}$, $0 \leq p_1 < p_2 < \dots < p_m$, $p_{m+1} \geq 0$, $0 \leq q_1 < q_2 < \dots < q_l$, $q_{l+1} \geq 0$, определяют одно и то же преобразование над множеством X^* тогда и только тогда, когда их правые части совпадают графически, т.е.

$$m = l, \quad \varepsilon_1 = \mu_1, \quad \varepsilon_2 = \mu_2, \quad p_i = q_i, \quad 1 \leq i \leq m.$$

ДОКАЗАТЕЛЬСТВО. Если правые части элементов s_1 и s_2 графически совпадают, то они, очевидно, определяют одно и то же преобразование над X^* . Поэтому достаточно показать, что, если s_1 и s_2 имеют различные приведенные виды, то они определяют разные преобразования над множеством X^* . Рассмотрим возможные случаи для значений ε_1 и μ_1 .

Случай 1. $\varepsilon_1 = 1$ и $\mu_1 = 1$. Полугрупповые слова s_1 и s_2 начинаются со слова $f_1 f_2$. Так как f_1 – биекция, то преобразования, заданные s_1 и s_2 , совпадают тогда и только тогда, когда совпадают преобразования $f_1^{-1} s_1 = f_1 s_1 = f_1^0 f_2 (f_1 f_2)^{p_1} \dots f_1^{\varepsilon_2}$ и $f_1^{-1} s_2 = f_1 s_2 = f_1^0 f_2 (f_1 f_2)^{q_1} \dots f_1^{\mu_2}$, что сводится к случаю $\varepsilon_1 = 0$ и $\mu_1 = 0$, который будет рассмотрен ниже.

Случай 2. $\varepsilon_1 = 1$ и $\mu_1 = 0$. Так как $m \geq 0$, то полугрупповые слова s_1 и s_2 начинаются с символов $f_1 f_2$ и f_2 соответственно. Для слова $u = b$ и s_1 имеем

$$s_1(b) = f_1 f_2 (f_1 f_2)^{p_1} \dots f_1^{\varepsilon_2}(b) = f_1 f_2 ((f_1 f_2)^{p_1} \dots f_1^{\varepsilon_2}(b)) = f_1(b) = a,$$

а для s_2 аналогично получаем

$$s_2(b) = f_2((f_1 f_2)^{q_1} \dots f_1^{\mu_2}(b)) = b.$$

Таким образом, в этом случае элементы s_1 и s_2 определяют разные преобразования над X^* . Аналогично рассматривается случай $\varepsilon_1 = 0$ и $\mu_1 = 1$.

Случай 3. $\varepsilon_1 = 0$ и $\mu_1 = 0$. Полугрупповые слова s_1 и s_2 начинаются с символов f_2 . Рассмотрим возможные случаи значений ε_2 и μ_2 .

3.а) Если $\varepsilon_2 = 0$ и $\mu_2 = 0$, то элементы s_1 и s_2 приводятся к следующему виду:

$$\begin{aligned} s_1 &= f_2(f_1 f_2)^{p_1} f_2(f_1 f_2)^{p_2} f_2 \dots (f_1 f_2)^{p_m} f_2(f_1 f_2)^{p_{m+1}}, \\ s_2 &= f_2(f_1 f_2)^{q_1} f_2(f_1 f_2)^{q_2} f_2 \dots (f_1 f_2)^{q_l} f_2(f_1 f_2)^{q_{l+1}}, \end{aligned} \quad (17)$$

где $0 \leq p_1 < p_2 < \dots < p_m, p_{m+1} \geq 0, 0 \leq q_1 < q_2 < \dots < q_l, q_{l+1} \geq 0, l, m \geq 0$. Положим для определенности $l \geq m \geq 0$ и индукцией по параметру l покажем, что s_1 и s_2 определяют разные преобразования над множеством X^* .

Пусть $l = 0$. Тогда $m = 0$ и элементы (17) имеют вид $s_1 = f_2(f_1 f_2)^{p_1}, s_2 = f_2(f_1 f_2)^{q_1}$. Если $p > 0$ – некоторое натуральное число, то из (7) имеем

$$f_2(f_1 f_2)^p = (f_2(f_1 f_2)^p, f_2(f_1 f_2)^{p-1})\sigma_b.$$

Отсюда для слова $u = b^{p+2}$ получаем

$$f_2(f_1 f_2)^p(b^{p+2}) = b \cdot f_2(f_1 f_2)^{p-1}(b^{p+1}) = \dots = b^p \cdot f_2(b^2) = b^{p+1} \cdot f_1(b) = b^{p+1}a, \quad (18)$$

а для слова $v = b^{q+2}$, где $q < p$, имеем

$$f_2(f_1 f_2)^p(b^{q+2}) = b \cdot f_2(f_1 f_2)^{p-1}(b^{q+1}) = \dots = b^q \cdot f_2(f_1 f_2)^{p-q}(b^2) = b^{q+2}. \quad (19)$$

Предположим, что $p_1 < q_1$. Для преобразований, задаваемых s_1 и s_2 , из (18) и (19) следуют равенства

$$s_1(b^{p_1+2}) = f_2(f_1 f_2)^{p_1}(b^{p_1+2}) = b^{p_1+1}a$$

и

$$s_2(b^{p_1+2}) = f_2(f_1 f_2)^{q_1}(b^{p_1+2}) = b^{p_1+2}.$$

Таким образом, элементы s_1 и s_2 определяют разные преобразования над X^* . Случай $p_1 > q_1$ рассматривается аналогично, а $p_1 = q_1$ не может выполняться, так как по предположению s_1 и s_2 имеют разный приведенный вид.

Пусть теперь $l > 1$. Рассмотрим элемент $s_3 \in S_A$ такой, что в его приведенном виде (12) $\varepsilon_i = 0, i = 1, 2$. Запишем его следующим образом:

$$\begin{aligned} s_3 &= f_2(f_1 f_2)^{t_1} f_2 \dots (f_1 f_2)^{t_n} f_2(f_1 f_2)^{t_{n+1}} \\ &= f_1(f_1 f_2)^{t_1+1} f_2(f_1 f_2)^{t_2} f_2 \dots (f_1 f_2)^{t_n} f_2(f_1 f_2)^{t_{n+1}}, \end{aligned}$$

где $0 \leq t_1 < t_2 < \dots < t_n, t_{n+1} \geq 0, n \geq 0$. Для слова $u = a^k v, |v| > 0, k \leq t_1 + 1$, из (6) и (7), построив развернутый вид преобразования s_3 , получаем

$$\begin{aligned} s_3(u) &= f_1(f_1 f_2)^{t_1+1} f_2(f_1 f_2)^{t_2} f_2 \dots (f_1 f_2)^{t_n} f_2(f_1 f_2)^{t_{n+1}}(a^k v) \\ &= b^k \cdot f_1(f_1 f_2)^{t_1+1-k} f_2(f_1 f_2)^{t_2-k} f_2 \dots (f_1 f_2)^{t_n-k} f_2(f_1 f_2)^{t_{n+1}}(v). \end{aligned} \quad (20)$$

Положим $k = \min(p_1, q_1) + 1$ и рассмотрим следующие элементы s_4 и s_5 полугруппы S_A :

$$\begin{aligned} s_4 &= f_1(f_1 f_2)^{p_1+1-k} f_2(f_1 f_2)^{p_2-k} f_2 \dots (f_1 f_2)^{p_m-k} f_2(f_1 f_2)^{p_{m+1}}, \\ s_5 &= f_1(f_1 f_2)^{q_1+1-k} f_2(f_1 f_2)^{q_2-k} f_2 \dots (f_1 f_2)^{q_l-k} f_2(f_1 f_2)^{q_{l+1}}. \end{aligned}$$

Для элементов s_1 и s_2 , заданных равенствами (17), из (20) имеем

$$\begin{aligned} s_1(u) &= b^k \cdot f_1(f_1 f_2)^{p_1+1-k} f_2(f_1 f_2)^{p_2-k} f_2 \dots (f_1 f_2)^{p_m-k} f_2(f_1 f_2)^{p_{m+1}}(v) = b^k \cdot s_4(v), \\ s_2(u) &= b^k \cdot f_1(f_1 f_2)^{q_1+1-k} f_2(f_1 f_2)^{q_2-k} f_2 \dots (f_1 f_2)^{q_l-k} f_2(f_1 f_2)^{q_{l+1}}(v) = b^k \cdot s_5(v). \end{aligned} \quad (21)$$

Предположим, что $p_1 = q_1$. Тогда оба числа $p_1 + 1 - k$ и $q_1 + 1 - k$ равны нулю. В этом случае элементы s_4 и s_5 имеют различный приведенный вид по выбору s_1 и s_2 и по предположению индукции определяют разные преобразования над множеством X^* . Пусть теперь $p_1 > q_1$ (случай $p_1 < q_1$ рассматривается аналогично). Тогда $p_1 + 1 - k > 0$ и $q_1 + 1 - k = 0$. В этом случае элемент s_4 имеет приведенный вид (12) при $\varepsilon_1 = 0$, а элемент s_5 – при $\varepsilon_1 = 1$. В п. 2 было показано, что тогда s_4 и s_5 не совпадают над X^* .

3.б) Пусть $\varepsilon_2 = 1$ и $\mu_2 = 1$. Так как f_1 – биекция, то элементы s_1 и s_2 определяют одинаковые преобразования тогда и только тогда, когда элементы $s_1 f_1$ и $s_2 f_1$ определяют одинаковые преобразования над множеством X^* . Поэтому этот случай сводится к случаю значений $\varepsilon_2 = 0$ и $\mu_2 = 0$, разобранному выше.

3.с) Пусть $\varepsilon_2 = 0$ и $\mu_2 = 1$ (случай $\varepsilon_2 = 1$ и $\mu_2 = 0$ рассматривается аналогично). Элементы s_1 и s_2 имеют следующий (различный) приведенный вид:

$$\begin{aligned} s_1 &= f_2(f_1 f_2)^{p_1} f_2(f_1 f_2)^{p_2} f_2 \dots (f_1 f_2)^{p_m} f_2(f_1 f_2)^{p_{m+1}}, \\ s_2 &= f_2(f_1 f_2)^{q_1} f_2(f_1 f_2)^{q_2} f_2 \dots (f_1 f_2)^{q_l} f_2(f_1 f_2)^{q_{l+1}} f_1, \end{aligned} \quad (22)$$

где $0 \leq p_1 < p_2 < \dots < p_m, p_{m+1} \geq 0, 0 \leq q_1 < q_2 < \dots < q_l, q_{l+1} \geq 0, l, m \geq 0$.

Предположим, что полугрупповые слова s_1 и s_2 , заданные (22), определяют одинаковые преобразования над X^* . Тогда одинаковые преобразования определяют и элементы $s_1 s_3$ и $s_2 s_3$, где $s_3 \in S_A$ – произвольный элемент.

Пусть $p_{m+1} > p_m$. Положим $s_3 = f_2$. Тогда

$$\begin{aligned} s_1 f_2 &= f_2(f_1 f_2)^{p_1} f_2(f_1 f_2)^{p_2} f_2 \dots (f_1 f_2)^{p_m} f_2(f_1 f_2)^{p_{m+1}} f_2, \\ s_2 f_2 &= f_2(f_1 f_2)^{q_1} f_2(f_1 f_2)^{q_2} f_2 \dots (f_1 f_2)^{q_l} f_2(f_1 f_2)^{q_{l+1}} f_1 f_2, \end{aligned}$$

причем $s_1 f_2$ и $s_2 f_2$ представлены в виде (12). При этом из 3.а) следует, что $p_1 = q_1$, $p_2 = q_2, \dots, p_{m+1} = q_l$, $q_{l+1} + 1 = 0$, а это противоречит условию $q_{l+1} \geq 0$.

Пусть теперь $0 \leq p_{m+1} \leq p_m$. Положим $s_3 = (f_2 f_1)^{p_{m+1}} f_2$. Тогда элемент $s_1 s_3$ сокращается до следующего вида:

$$\begin{aligned} s_1 (f_2 f_1)^{p_{m+1}} f_2 &= f_2(f_1 f_2)^{p_1} \dots f_2(f_1 f_2)^{p_m} f_2(f_1 f_2)^{p_{m+1}} (f_2 f_1)^{p_{m+1}} f_2 \\ &= f_2(f_1 f_2)^{p_1} \dots f_2(f_1 f_2)^{p_m} f_2(f_1 f_2)^{p_{m+1}-1} (f_2 f_1)^{p_{m+1}-1} f_2 = \dots \\ &= f_2(f_1 f_2)^{p_1} \dots f_2(f_1 f_2)^{p_m} f_2 f_2 \\ &= f_2(f_1 f_2)^{p_1} \dots f_2(f_1 f_2)^{p_{m-1}} f_2(f_1 f_2)^{p_m}, \end{aligned}$$

а $s_2 s_3$ сразу имеет приведенный вид

$$\begin{aligned} s_2 (f_2 f_1)^{p_{m+1}} f_2 &= f_2(f_1 f_2)^{q_1} \dots f_2(f_1 f_2)^{q_l} f_2(f_1 f_2)^{q_{l+1}} f_1 (f_2 f_1)^{p_{m+1}} f_2 \\ &= f_2(f_1 f_2)^{q_1} \dots f_2(f_1 f_2)^{q_{l-1}} f_2(f_1 f_2)^{q_l} f_2(f_1 f_2)^{q_{l+1}+p_{m+1}+1}. \end{aligned}$$

В этом случае из 3.а) следует, что $m = l + 1$, $p_1 = q_1$, $p_2 = q_2, \dots, p_{m-1} = q_l$, $p_m = q_{l+1} + p_{m+1} + 1$.

Так как f_1 – биекция, то аналогичные рассуждения можно провести и для элементов $s_1 f_1$ и $s_2 f_1$, причем при этом s_1 и s_2 меняются местами. В случае $q_{l+1} > q_l$ получаем противоречие с условием $p_{m+1} \geq 0$, а в случае $0 \leq q_{l+1} \leq q_l$ имеем условия $q_1 = p_1$, $q_2 = p_2, \dots, q_{l-1} = p_m$, $q_l = p_{m+1} + q_{l+1} + 1$, что противоречит полученному ранее условию $m = l + 1$.

Таким образом, получили противоречие с тем, что s_1 и s_2 , заданные (22), определяют одно и то же преобразование над множеством X^* .

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1. По лемме 5 в полугруппе S_A выполняются соотношения системы (11). Для доказательства первой части теоремы достаточно показать, что любые два полугрупповых слова в алфавите f_1, f_2 либо переводятся друг в друга соотношениями из (11), либо определяют различные преобразования над X^* .

По лемме 6 с помощью соотношений $f_1^2 = \text{Id}$ и $r_k, k \geq 0$, любое полугрупповое слово s можно привести к виду (12). Заметим, что вид (12) определяется однозначно. Для этого проверим, что произвольные элементы s_1 и s_2 полугруппы S_A , имеющие различный приведенный вид, определяют разные преобразования над множеством X^* .

Если s_1, s_2 такие, что в приведенном виде (12) каждого из них $m \geq 0$, то они определяют различные преобразования над множеством X^* в силу леммы 7. Если для приведенного вида s_1 и s_2 выполняется условие $m = -1$, то по лемме 6 они равны элементам Id и f_1 , которые определяют различные преобразования над X^* .

Пусть, наконец, элементы s_1 и s_2 таковы, что для приведенного вида одного из них (например, s_1) выполняется условие $m = -1$, а для приведенного вида другого (например, s_2) – условие $m \geq 0$. Тогда преобразование, определяемое s_2 , не будет биекцией над множеством X^* и поэтому не совпадает с s_1 .

Таким образом, два элемента s_1 и s_2 определяют одно и то же преобразование над X^* тогда и только тогда, когда они с помощью соотношений системы (11) приводятся к одному и тому же приведенному виду (12). Отсюда следует, что полугруппа S_A имеет задание образующими и определяющими соотношениями, указанное в (1).

Для решения проблемы равенства слов s_1 и s_2 в полугруппе S_A требуется привести эти слова к виду (12), а затем проверить их на графическое равенство. Так как по лемме 6 эти слова сводятся к приведенному виду за $\lceil |s_1|/2 \rceil + \lceil |s_2|/2 \rceil$ шагов, то проблема равенства слов в полугруппе S_A решается за линейное время.

4. Доказательство теоремы 2. Обозначим количество всех несократимых элементов длины l полугруппы S_A символом $w(l)$, а количество несократимых слов, которые начинаются символом f_i , $i = 1, 2$, как $w_i(l)$. Заметим, что для $l \geq 2$

$$w(l) = w_1(l) + w_2(l) = w_2(l-1) + w_2(l). \quad (23)$$

Кроме того, $w(1) = 2$, $w(2) = 4$ и положим $w_2(1) = 2$. Найдем значение числа $w_2(l)$

ЛЕММА 8. Для любого натурального числа $l \geq 2$ имеет место равенство

$$w_2(l) = \sum_{m=1}^{\lfloor \sqrt{l-1} \rfloor} \sum_{p=m}^{d(l-1, m)} R_{p, m} + 1, \quad (24)$$

где $d(l, m) = \lfloor \frac{1}{2}((l+1) - (m-1)^2) \rfloor$.

ДОКАЗАТЕЛЬСТВО. Пусть $l \geq 2$ – фиксированное натуральное число. По определению $w_2(l)$ равно количеству элементов вида (12), для которых выполняются условия

$$m \geq 0, \quad \varepsilon_1 = 0, \quad 0 \leq p_1 < p_2 < p_3 < \dots < p_m, \quad p_{m+1} \geq 0$$

и

$$2 \sum_{i=1}^{m+1} p_i + (m+1) + \varepsilon_2 = l. \quad (25)$$

Если значения параметров m и $p_1, p_2, \dots, p_m$ фиксированы, то согласно (25) параметры p_{m+1} и ε_2 однозначно определяются формулами

$$p_{m+1} = \left\lfloor \frac{1}{2} \left(l - (m+1) - 2 \sum_{i=1}^m p_i \right) \right\rfloor \quad \text{и} \quad \varepsilon_2 = \left(l - (m+1) - 2 \sum_{i=1}^m p_i \right) - 2p_{m+1},$$

где $\lfloor x \rfloor$ – целая часть числа x . Поэтому число $w_2(l)$ равно количеству различных значений параметров m и $p_1, p_2, \dots, p_m$, удовлетворяющих условию

$$2 \sum_{i=1}^m p_i + m \leq l-1. \quad (26)$$

Для каждого значения m минимальные значения параметров $p_1, p_2, \dots, p_m$ равны соответственно $0, 1, \dots, m-1$, и поэтому параметр m изменяется в пределах от 0 до $[\sqrt{l-1}]$, так как из (26) имеем

$$l-1 \geq m+2 \sum_{i=1}^m p_i \geq m+2 \sum_{i=1}^m (i-1) = m+2 \frac{m(m-1)}{2} = m^2.$$

Пусть параметр m зафиксирован. Если $m=0$, то существует единственный элемент полугруппы, удовлетворяющий условию (26). Если $m>0$, то значение суммы $p = \sum_{i=1}^m p_i$ изменяется от $\sum_{i=1}^m (i-1) = m(m-1)/2$ до $[(l-m-1)/2]$. Для каждого значения p число различных значений параметров $p_1, p_2, \dots, p_m$ равно $V_{p,m}$ – количеству разбиений числа p на m различных неотрицательных слагаемых. Отсюда получаем следующее равенство:

$$w_2(l) = \sum_{m=1}^{[\sqrt{l-1}]} \sum_{p=m(m-1)/2}^{[(l-m-1)/2]} V_{p,m} + 1.$$

Воспользовавшись тем, что $V_{p+m(m-1)/2,m} = R_{p+m,m}$ (см. [23, с. 268]), преобразуем внутреннюю сумму

$$\begin{aligned} \sum_{p=m(m-1)/2}^{[(l-m-1)/2]} V_{p,m} &= \sum_{p=0}^{[(l-m-1)/2]-m(m-1)/2} V_{p+m(m-1)/2,m} = \sum_{p=0}^{[(l-m^2-1)/2]} R_{p+m,m} \\ &= \sum_{p=m}^{[(l-(m-1)^2)/2]} R_{p,m} = \sum_{p=m}^{d(l-1,m)} R_{p,m}, \end{aligned}$$

откуда получаем равенство (24), и лемма доказана.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2. Так как для любого $n \in \mathbb{N}$ по определению

$$\gamma_S(n) = \sum_{l=1}^n w(l),$$

то по лемме 8 из (23) и (24) имеем

$$\begin{aligned} \gamma_S(n) &= 4 + 2 \sum_{l=2}^{n-1} w_2(l) + w_n(l) \\ &= 1 + 2n + 2 \sum_{l=2}^{n-1} \sum_{m=1}^{[\sqrt{l-1}]} \sum_{p=m}^{d(l-1,m)} R_{p,m} + \sum_{m=1}^{[\sqrt{n-1}]} \sum_{p=m}^{d(n-1,m)} R_{p,m} \\ &= (2n+1) + 2 \sum_{l=1}^{n-2} \sum_{m=1}^{[\sqrt{l}]} \sum_{p=m}^{d(l,m)} R_{p,m} + \sum_{m=1}^{[\sqrt{n-1}]} \sum_{p=m}^{d(n-1,m)} R_{p,m}, \end{aligned}$$

и теорема 2 доказана.

Для доказательства следствия потребуется несколько лемм.

ЛЕММА 9. Для функции $\gamma_S(n)$ при $n \geq 3$ выполняются неравенства

$$2 \sum_{l=1}^{n-2} \sum_{p=1}^{[\sqrt{l}]} R_p + \sum_{p=1}^{[\sqrt{n-1}]} R_p \leq \gamma_S(n) - (2n+1) \leq 2 \sum_{l=2}^{n-1} \sum_{p=1}^{[l/2]} R_p + \sum_{p=1}^{[n/2]} R_p.$$

ДОКАЗАТЕЛЬСТВО. Учитывая (2), достаточно показать, что имеют место неравенства

$$\sum_{p=1}^{[\sqrt{l}]} R_p \leq \sum_{m=1}^{[\sqrt{l}]} \sum_{p=m}^{d(l,m)} R_{p,m} \leq \sum_{p=1}^{[(l+1)/2]} R_p. \quad (27)$$

Для этого во внутренней сумме неравенств (27) поменяем местами индексы и разложим ее на три части:

$$\sum_{m=1}^{[\sqrt{l}]} \sum_{p=m}^{d(l,m)} R_{p,m} = \sum_{p=1}^{[\sqrt{l}]} \sum_{m=1}^p R_{p,m} + \sum_{p \in P_1} \sum_{m=1}^{[\sqrt{l}]} R_{p,m} + \sum_{p \in P_2} \sum_{m=1}^{[\sqrt{l+1-2p}]+1} R_{p,m}, \quad (28)$$

где

$$P_1 = \left\{ p \mid [\sqrt{l}] < p < [\sqrt{l}] + \left\lfloor \frac{1}{2}(l - [\sqrt{l}]^2) \right\rfloor \right\},$$

$$P_2 = \left\{ p \mid [\sqrt{l}] + \left\lfloor \frac{1}{2}(l - [\sqrt{l}]^2) \right\rfloor \leq p \leq \left\lfloor \frac{1}{2}(l+1) \right\rfloor \right\},$$

и соответствующая сумма равна нулю, если P_i – пустое множество, $i = 1, 2$. Так как $R_{p,m} = 0$ при $m > p$, то

$$R_p = \sum_{m \geq 1} R_{p,m} = \sum_{m=1}^p R_{p,m}.$$

Тогда из (28) следуют неравенства (27), и лемма доказана.

ЛЕММА 10 [12]. Пусть c – некоторое ненулевое число. Для достаточно больших N имеет место соотношение

$$\sum_{n=1}^N n^\alpha e^{c\sqrt{n}} = \frac{2}{c} N^{\alpha+1/2} e^{c\sqrt{N}} + O(N^{\alpha+1/2} e^{c\sqrt{N}}).$$

ДОКАЗАТЕЛЬСТВО. Достаточно применить интегрирование по частям в формуле суммирования Эйлера–Маклорена.

Аналогично проверяется, что имеет место

ЛЕММА 11. Для достаточно больших N справедливо соотношение

$$\sum_{n=1}^N n^\alpha e^{c\sqrt[4]{n}} = \frac{4}{c} N^{\alpha+3/4} e^{c\sqrt[4]{N}} + O(N^{\alpha+3/4} e^{c\sqrt[4]{N}}).$$

Из асимптотической формулы Харди–Рамануджана для R_p (см. [22], а также [23, с. 271]) следует, что для любого $\varepsilon > 0$ при достаточно больших p имеют место неравенства

$$\frac{1-\varepsilon}{4p\sqrt{3}} e^{\pi\sqrt{2p/3}} < R_p < \frac{1+\varepsilon}{4p\sqrt{3}} e^{\pi\sqrt{2p/3}}. \quad (29)$$

ДОКАЗАТЕЛЬСТВО СЛЕДСТВИЯ. 1. *Верхняя оценка.* По лемме 9 имеем

$$\gamma_S(n) - (2n + 1) \leq 2 \sum_{l=2}^{n-1} \sum_{p=1}^{[l/2]} R_p + \sum_{p=1}^{[n/2]} R_p.$$

Из (29) и леммы 10 следует, что при достаточно больших p_0 выполняется неравенство

$$\sum_{p=1}^{p_0} R_p < \frac{1+\varepsilon}{4\sqrt{3}} \sum_{p=1}^{p_0} p^{-1} e^{\pi\sqrt{2/3}\sqrt{p}} \leq \frac{1+\varepsilon}{2\pi\sqrt{2}} p_0^{-1/2} e^{\pi\sqrt{2/3}\sqrt{p_0}},$$

откуда

$$\gamma_S(n) - (2n + 1) \leq \frac{1+\varepsilon}{2\pi\sqrt{2}} \left(2 \sum_{l=2}^{n-1} \left(\frac{l}{2} \right)^{-1/2} e^{\pi\sqrt{2/3}\sqrt{l/2}} + \left(\frac{n}{2} \right)^{-1/2} e^{\pi\sqrt{2/3}\sqrt{n/2}} \right).$$

Еще раз применив к последнему неравенству лемму 10, получаем правую часть оценки (3):

$$\begin{aligned} \gamma_S(n) - (2n + 1) &\leq \frac{1+\varepsilon}{2\pi} \left(\frac{4\sqrt{3}}{\pi} e^{\pi\sqrt{n-1}/\sqrt{3}} + n^{-1/2} e^{\pi\sqrt{n}/\sqrt{3}} \right) \\ &< \frac{1+\varepsilon}{2\pi} e^{\pi\sqrt{n}/\sqrt{3}} \left(\frac{4\sqrt{3}}{\pi} + n^{-1/2} \right). \end{aligned}$$

2. *Нижняя оценка.* По лемме 9 имеем также

$$2 \sum_{l=1}^{n-2} \sum_{p=1}^{[\sqrt{l}]} R_p + \sum_{p=1}^{[\sqrt{n-1}]} R_p \leq \gamma_S(n) - (2n + 1).$$

Из (29) и леммы 10 следует, что при достаточно больших p_0 имеет место

$$\sum_{p=1}^{p_0} R_p > \frac{1-\varepsilon}{4\sqrt{3}} \sum_{p=1}^{p_0} p^{-1} e^{\pi\sqrt{2/3}\sqrt{p}} \geq \frac{1-\varepsilon}{2\pi\sqrt{2}} p_0^{-1/2} e^{\pi\sqrt{2/3}\sqrt{p_0}},$$

откуда

$$\gamma_S(n) - (2n + 1) \geq \frac{1-\varepsilon}{2\pi\sqrt{2}} \left(2 \sum_{l=1}^{n-2} (\sqrt{l})^{-1/2} e^{\pi\sqrt{2/3}\sqrt[4]{l}} + (\sqrt{n-1})^{-1/2} e^{\pi\sqrt{2/3}\sqrt[4]{n-1}} \right).$$

Применив лемму 11 к правой части последнего неравенства, получаем левую часть оценки (3):

$$\begin{aligned} \gamma_S(n) - (2n + 1) &\geq \frac{1-\varepsilon}{2\pi\sqrt{2}} \left(\frac{8\sqrt{3}}{\pi\sqrt{2}} \sqrt{n-2} e^{\pi\sqrt{2/3}\sqrt[4]{n-2}} + \frac{e^{\pi\sqrt{2/3}\sqrt[4]{n-1}}}{\sqrt[4]{n-1}} \right) \\ &\geq \frac{1-\varepsilon}{2\pi\sqrt{2}} \sqrt{n-2} e^{\pi\sqrt{2/3}\sqrt[4]{n-2}} \left(\frac{4\sqrt{6}}{\pi} + (n-2)^{-3/4} \right). \end{aligned}$$

Переходя к порядкам роста в оценке (3), получаем соотношение (4), и следствие полностью доказано.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] Уфнаровский В. А. Комбинаторные и асимптотические методы в алгебре // Итоги науки и техники. Современные проблемы математики. Фундаментальные направления. Т. 57. М.: ВИНТИ, 1990. С. 5–177.
- [2] Бабенко И. К. Проблемы роста и рациональности в алгебре и топологии // УМН. 1986. Т. 41. № 2. С. 95–142.
- [3] Шварц А. С. Объемные инварианты покрытий // Докл. АН СССР. 1955. Т. 105. С. 32–34.
- [4] Milnor J. A note on curvature and fundamental groups // J. Differential Geometry. 1968. V. 2. P. 1–7.
- [5] Milnor J. Growth of finitely generated solvable groups // J. Differential Geometry. 1968. V. 2. № 4. P. 447–451.
- [6] Wolf J. Growth of finitely generated solvable groups and curvature of Riemannian manifolds // J. Differential Geometry. 1968. V. 2. № 4. P. 421–446.
- [7] Gromov M. Groups of polynomial growth and expanding maps // Publ. Math. Inst. Hautes Etudes Sci. 1981. V. 53. P. 53–73.
- [8] Григорчук Р. И. О полугруппах с сокращениями степенного роста // Матем. заметки. 1988. Т. 43. № 3. С. 305–319.
- [9] Григорчук Р. И. Степени роста конечно-порожденных групп и теория инвариантных средних // Изв. АН СССР. Сер. матем. 1984. Т. 48. № 5. С. 939–985.
- [10] Григорчук Р. И. Строение p -групп промежуточного роста, имеющих континуум фактор-групп // Алгебра и логика. 1984. Т. 23. № 4. С. 383–394.
- [11] Беляев В. В., Сесекин Н. Ф., Трофимов В. И. Функции роста полугрупп и луп // Записки Уральского гос. ун-та. 1977. Т. 10. № 3. С. 3–8.
- [12] Lavrik-Mannlin A. A. On some semigroups of intermediate growth // Preprint of Department of Mathematics. Switzerland: ETH Zurich, 2001.
- [13] Okninski J. Semigroups of Matrices. Singapore: World Scientific, 1988.
- [14] Shneerson L. M. Relatively free semigroups of intermediate growth // J. Algebra. 2001. V. 235. P. 484–546.
- [15] Grigorchuk R. I. Growth and amenability of a semigroup and its group of quotients // Proceedings of the International Symposium on the Semigroup Theory. Kyoto, 1990. P. 103–108.
- [16] Fabrykowski J., Gupta N. On groups with sub-exponential growth functions. II // J. Indian Math. Soc. 1991. V. 56. № 1–4. P. 217–228.
- [17] Григорчук Р. И., Некрашевич В. В., Сущанский В. И. Автоматы, динамические системы и группы // Тр. МИАН. 2000. Т. 231. С. 134–214.
- [18] Bartholdi L. Croissance de groupes agissant sur des arbres. PhD Dissertation. Geneve: Univ. Geneve, 2000.
- [19] Резников И. И., Сущанский В. И. О функциях роста полугрупп, определенных автоматами Мили с двумя состояниями над двухбуквенным алфавитом // Праці Третьої Міжнародної Алгебраїчної конференції в Україні. Суми, 2001. С. 238–239.
- [20] Резников И. И., Сущанский В. И. Функции роста автоматов с двумя состояниями над двухэлементным алфавитом // Доповіді НАН України. 2002. № 1.
- [21] Резников И. И. Автоматы Мили с двумя состояниями над двухбуквенным алфавитом, которые порождают свободную полугруппу // Вісник Київського університету. 2001. № 3. С. 91–98.
- [22] Hardy G. H., Ramanujan S. Asymptotic formulae in combinatory analysis // Proc. London Math. Soc. 1918. V. 17. № 2. P. 75–115.
- [23] Сачков В. Н. Комбинаторные методы дискретной математики. М.: Наука, 1977.
- [24] Биркгоф Г., Барти Т. Современная прикладная алгебра. М.: Мир, 1976.
- [25] Глушков В. М. Абстрактная теория автоматов // УМН. 1961. Т. 16. № 5. С. 3–62.

(И. И. Резников) Киевский национальный университет им. Тараса Шевченко
(В. И. Сущанский) Силезский технический университет

Поступило
10.03.2001