

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
имени М. В. ЛОМОНОСОВА

Механико-математический факультет

На правах рукописи

Иванов-Погодаев Илья Анатольевич

УДК 512.552 512.532

Машина Минского, свойства нильпотентности и размерность  
Гельфанда-Кириллова в конечно-определенных полугруппах

01.01.06 — математическая логика, алгебра и теория чисел

Диссертация на соискание ученой степени  
кандидата физико-математических наук

Научный руководители:  
доктор физико-математических наук,  
профессор А. В. Михалев  
доктор физико-математических наук,  
А. Я. Белов

Москва — 2006

## Оглавление

<i>Введение</i>	4
1. Алгебра с конечным базисом Грёбнера, и неразрешимой проблемой делителей нуля	9
1.1 План построения алгебры с идеалом соотношений, заданным конечным базисом Грёбнера, в которой вопрос, является ли элемент делителем нуля, алгоритмически неразрешим	9
1.2 Универсальная машина Тьюринга и определяющие соотношения	12
1.3 Делители нуля и остановка машины	14
2. Вспомогательные сведения о машине Минского	26
3. Реализация Машины Минского в конечно-определенной полугруппе	35
3.1 План построения полугруппы с полуцелой размерностью Гельфанд–Кириллова	35
3.2 Определяющие соотношения	36
3.3 Приведение к каноническому виду	38
3.4 Работа основного механизма	43
3.5 Система инвариантов	46
3.6 Преобразование для увеличения количества нормальных слов	51
4. Построение полугруппы с рекурсивной размерностью Гельфанд–Кириллова	52
4.1 План построения полугруппы с рекурсивной размерностью Гельфанд–Кириллова	52
4.2 Определяющие соотношения	54
4.3 Приведение к каноническому виду	55
4.4 Система инвариантов	60

4.5	Присоединение . . . . .	63
4.6	Создание машины Минского в полугруппе . . . . .	65
5.	Конструкция конечно-определенной полугруппы, содержащей ненильпотентный ниль-идеал . . . . .	69
	<i>Библиография</i> . . . . .	76

## ВВЕДЕНИЕ

Широко известна бернсайдова проблематика, охватывающая большой круг вопросов, как в теории групп, так и в смежных областях. Проблемам бернсайдовского типа посвящена обзорная статья Е.И.Зельманова [20]. В *PI*-случае вопросы локальной конечности алгебраических алгебр решаются положительно. В ассоциативном случае соответствующий результат был получен И.Капланским и Д.Левицким. Чисто комбинаторное доказательство для ассоциативного случая получается из теоремы Ширшова о высоте [21], [22]. Для *PI*-алгебр Ли соответствующий результат был получен Е.И.Зельмановым и А.И.Кострикиным. Подробная библиография по этому вопросу изложена в монографии [24].

Первый контрпример к “неограниченной” проблеме был найден Е. С. Голодом в 1964 году на основе универсальной конструкции Е. С. Голода– И. Р. Шафаревича. Вопрос о локальной конечности групп с тождеством  $x^n = 1$  был решен отрицательно в знаменитых работах П. С. Новикова и С. И. Адяна [1968]: было доказано существование для любого нечетного  $n \geqslant 4381$  бесконечной группы с  $t > 1$  образующими, удовлетворяющей тождеству  $x^n = 1$ . Эта оценка была улучшена до  $n \geqslant 665$  С. И. Адяном [1975]. Позднее А. Ю. Ольшанский предложил геометрически наглядный вариант доказательства для нечетных  $n > 10^{10}$ . В конечно-определенном случае все подобные вопросы сильно усложняются. В этом направлении работают многие исследователи, и определенного прогресса достигли М. Сапир и И. Рипс.

Построения в группах, как правило, более сложны, чем в полугруппах. Например, вопрос о существовании конечно-порожденной нильполугруппы, то есть полугруппы, каждый элемент которой в некоторой степени обращается в нуль, имеет тривиальный положительный ответ: уже в алфавите из двух букв имеются слова сколь угодно большой длины, не содержащие трех подряд одинаковых подслов (кубов). Первая конструкция такого рода принадлежит Туэ [1912]. Однако, если потребовать от полугруппы возможность ее задания конечным числом определяющих соотношений, ситуация сильно усложняется – вопрос о суще-

ствовании такой полугруппы открыт (см. [Свердловская Тетрадь]).

На проблематику, связанную с построением разного рода экзотических объектов с помощью конечного числа определяющих соотношений обратил внимание В. Н. Латышев. Им же была поставлена проблема существования конечно определенного ниль-кольца [23].

В качестве продвижения в решении этого вопроса можно рассматривать результаты Хигмана, Г. П. Кукина, В. Я. Беляева о вложениях рекурсивно-определеных объектов в конечно-определенные. [7], [9], в частности, теорема Хигмана о вложении рекурсивно-определеных групп в конечно-определенные. В этом контексте можно рассматривать результат о существовании конечно-определенной полугруппы, содержащей ненильпотентный ниль-идеал, рассматриваемый в настоящей диссертации.

Хотя до сих пор и не удается построить контрпримеры к проблемам Бернсайдовского типа с помощью конечного набора определяющих соотношений, были построены конечно определенные объекты с разного рода “экзотическими” свойствами. В. А. Уфнаровским был построен пример конечно-определенной алгебры с промежуточным ростом [3]. Этот пример представляет собой универсальную обертывающую алгебру алгебры Ли со степенным ростом. В данной диссертации приведена конструкция конечно определенной полугруппы с нецелой размерностью Гельфанд-Кириллова.

Для построения конечно-определенных полугрупп с подобными “экзотическими” свойствами чрезвычайно эффективным оказывается подход, связанный с использованием машины Минского. Машина Минского эквивалентна *Машине Тьюринга*, но в ее конструкции используется только два регистра. Этим объясняется ее удобство при использовании в алгебраических конечно-определенных системах.

В настоящей диссертации данный подход используется для построения конечно-определенной полугруппы с размерностью Гельфанд-Кириллова, равной  $N + \alpha$ , где  $\alpha$  – некоторое рекурсивное число,  $N$  – натуральное число, зависящее от  $\alpha$ . В процессе построения в полугруппе реализуется машина Минского, вычисляющая соответствующее рекурсивное  $\alpha$ . Кроме того, система соотношений определяет канонический вид слова для реализации требуемой размерности Гельфанд-Кириллова.

Построение разного рода конечно определенных экзотических объектов тесно связано с алгоритмической проблематикой. Известно, что про-

блема равенства в конечно-определенной полугруппе, а следовательно, и алгебре, алгоритмически неразрешима. С другой стороны, эта проблема разрешима, если идеал соотношений задан конечным базисом Грёбнера, замкнутым относительно композиции [12]. В этой связи В. Н. Латышев в 1980 году поставил опрос о существовании алгоритма определения, является ли данный элемент делителем нуля или нильпотентом в случае, когда идеал соотношений задан конечным базисом Грёбнера.

Кроме этого, В. Н. Латышевым был поставлен также аналогичный вопрос для мономиальных автоматных алгебр. Для этого случая существование алгоритма проверки, является ли данный элемент нильпотентом, было установлено В. В. Борисенко, а существование алгоритма для делителей нуля – А. Я. Беловым и В. В. Борисенко [2]. Аналогичный результат для некоторого класса квадратичных алгебр был получен Н. К. Ильину [13], [14] а также Д. И. Пионтковским [15]. Все эти результаты вытекают из разрешимости системы линейных рекурентов на дереве [17]. Из результата работы [17] вытекает также существование алгоритма для установления делителей нуля для целого класса алгебр с *ограниченной переработкой* (аналогичной условию *малых сокращений* в теории групп).

**Определение 0.0.1.** Пусть на мономах алгебры  $A$  с фиксированной системой образующих есть порядок, для которого существует *нормальный базис*, т.е. базис из мономов, не представимых в виде линейной комбинации меньших. Алгебра  $A$  называется *алгеброй с ограниченной переработкой справа*, если при некотором  $d \in \mathbb{N}$  для любого нормального слова  $W$  в алгебре  $A$  и любой образующей  $a_i$  выполняется равенство

$$Wa_i = \bar{W} \cdot \left( \sum_j \lambda_{ij} W_j \right) \quad (0.1)$$

где  $\lambda_j \in \mathbb{F}$  для всех  $j$ , кроме того,  $WW_j$  суть нормальные слова алгебры  $A$ ,  $|W_j| \leq d$ , а слово  $\bar{W}$  есть начальный кусок слова  $W$  длины  $|W| - d$ .

Если множество слов нормального базиса образует регулярный язык, каждому слову отвечает вершина автомата и все коэффициенты  $\lambda_{ij}$  зависят только от типа вершины графа, отвечающего слову  $W$ , то  $A$  есть *автоматная алгебра с ограниченной переработкой справа*.

Аналогичным образом определяется (*автоматная*) алгебра с *ограниченной переработкой слева*.

Один из основных результатов данной диссертации показывает, что условие ограниченной переработки является необходимым. Мы стро-

им алгебру с алгоритмически неразрешимой проблемой делителей нуля, и идеалом соотношений, заданным конечным базисом Грёбнера. Тем самым дается отрицательный ответ на вопрос, поставленный В.Н.Латышевым.

Построение основано на подходе, связанным с использованием машины Минского. Для этого в полугруппе конструируется машина Минского, реализующая универсальную машину Тьюринга, одна элементарная операция работы которой соответствует умножению слева на выделенную букву. Остановка машины соответствует обнулению слова.

Таким образом, **основные результаты** диссертации таковы:

1. Построен пример алгебры, идеал соотношений которой задан конечным базисом Грёбнера, в которой вопрос, является ли элемент делителем нуля, алгоритмически неразрешим.
2. Построен пример конечно-определенной полугруппы с рекурсивной размерностью Гельфанд-Кириллова.
3. Построен пример бесконечной конечно-определенной полугруппы, содержащей ненильпотентный нильидеал.

**Методы исследования.** В работе использованы методы построения полугрупп с нулём и полугрупповых алгебр, с помощью введения определяющих соотношений. Основным элементом конструкции является реализация машины Минского. В первой главе реализуется универсальная машина для доказательства алгоритмической неразрешимости. При построении полугрупп с нецелой и рекурсивной размерностью Гельфанд-Кириллова машина используется как вычисляющий инструмент.

**Практическая и теоретическая ценность.** Работа носит теорети-

ческий характер.

**Апробация работы.** Основные результаты диссертации многократно докладывались на семинаре "Кольца и модули" кафедры высшей алгебры МГУ в 2000-2006 гг., а также на следующих конференциях:

1. Международная алгебраическая конференция в честь Е. С. Ляпина, Санкт-Петербург, 1999.
2. 65-th International Workshop in Algebra (AAA65) and Conference of Young Algebraists (CYA), Potsdam University, 2003.

Часть результатов опубликована в работе [10], автору диссертации принадлежит часть, относящаяся введению определяющих соотношений реализующих конструкцию обмена сигналами.

Отдельная часть результатов опубликована в статье [11], автору принадлежит часть, относящаяся к введению определяющих соотношений.

Основные результаты также опубликованы в сборниках тезисов докладов на международных конференциях (см. [??]).

**Структура диссертации.** Диссертация состоит из оглавления, введения, пяти глав и списка литературы, который включает 25 наименований.

**Благодарности.** Автор глубоко благодарен своим научным руководителям — доктору физико-математических наук профессору Алексею Яковлевичу Белову и доктору физико-математических наук Александру Васильевичу Михалеву за постановку задач, обсуждение результатов и постоянное внимание к работе.

Также автор хотел бы поблагодарить за внимание и обсуждения работы доктора физико-математических наук, профессора Латышева Виктора Николаевича, и доктора физико-математических наук, профессора Артамонова Вячеслава Александровича.

Автор выражает свою отдельную благодарность кандидату физико-математических наук Богданову Илье Игоревичу за детальное обсуждение работы.

# 1. АЛГЕБРА С КОНЕЧНЫМ БАЗИСОМ ГРЁБНЕРА, И НЕРАЗРЕШИМОЙ ПРОБЛЕМОЙ ДЕЛИТЕЛЕЙ НУЛЯ

## 1.1 План построения алгебры с идеалом соотношений, заданным конечным базисом Грёбнера, в которой вопрос, является ли элемент делителем нуля, алгоритмически неразрешим

Пусть  $\mathbb{A}$  – алгебра над полем  $\mathbb{K}$ . Фиксируем конечный алфавит образующих  $\{a_1, \dots, a_N\}$ . Словом в алгебре называется слово в алфавите образующих. Порядку на образующих отвечает лексикографический порядок на множестве слов.

Слова в алфавите образуют полугруппу. Основной идеей построения является реализация универсальной машины Тьюринга в этой полугруппе с помощью определяющих соотношений. Мы будем использовать универсальную машину Тьюринга, построенную М. Минским. Данная машина имеет 7 состояний и использует четырехцветную ленту. Она полностью задается 28 инструкциями, 27 из которых имеют вид:

$$(i, j) \rightarrow (L, q(i, j), t(i, j)) \text{ или } (i, j) \rightarrow (R, q(i, j), t(i, j)),$$

где  $0 \leq i \leq 6$  – текущее состояние машины,  $0 \leq j \leq 3$  – цвет текущей клетки,  $L$  или  $R$ , (налево или направо) – направление сдвига головки машины после выполнения данной инструкции,  $q(i, j)$  – состояние, в которое переходит машина после выполнения данной инструкции,  $t(i, j)$  – цвет, в который красится текущая клетка (из которой головка уходит).

Таким образом, инструкция  $(2, 3) \rightarrow (L, 3, 1)$  означает следующее: “Если головка машины – в клетке цвета 3 и состояние машины – 2, клетка перекрашивается в цвет 1, головка перемещается на одну клетку влево, машина переходит в состояние 3”.

Последняя инструкция –  $(4, 3) \rightarrow \text{СТОП}$ , то есть, если машина в состоянии 5, текущая клетка имеет цвет 3, машина заканчивает работу.

Для обозначения семи состояний головки машины будем использовать буквы  $Q_i$ ,  $0 \leq i \leq 6$ . Для обозначения цвета текущей клетки будем использовать буквы  $P_j$ , где  $0 \leq j \leq 3$ .

Действие машины Тьюринга зависит от текущего состояния  $Q_i$  и цвета текущей ячейки  $P_j$ . То есть, каждой паре  $Q_i$  и  $P_j$  соответствует одна инструкция машины Тьюринга.

Назовем инструкции, сдвигающие головку влево – левыми, а сдвигающие вправо – правыми. Таким образом, у нас есть левые пары  $(i, j)$ , соответствующие левым инструкциям, правые пары, соответствующие правым инструкциям и инструкция СТОП, соответствующая паре  $(4, 3)$ . Для обозначения левого направления движения в текущий момент, будем использовать букву  $M_0$ , для обозначения правого – букву  $M_1$ .

Будем считать *непустыми клетками* все клетки не нулевого цвета.

Таким образом, имеется два конечных куска ленты, слева и справа от текущей клетки. Пусть  $u_0, u_1, \dots, u_x$  – цвета клеток, (справа налево) начиная с ячейки слева от текущей. Таким образом,  $u_x$  – цвет крайней слева непустой ячейки (не первого цвета). Аналогично, пусть  $v_0, v_1, \dots, v_y$  – цвета клеток, (слева направо) начиная с ячейки справа от текущей.  $v_y$  – цвет крайней справа непустой ячейки.

Пусть  $k = u_04^0 + u_14^1 + \dots + u_x4^x$ ,  $n = v_04^0 + v_14^1 + \dots + v_y4^y$ . Для хранения  $k$  будем использовать степени  $a$  и  $c$ . Для хранения  $n$  – степени  $b$  и  $d$ .

Перекрашивание клеток и движение головки мы будем моделировать с помощью вычислений с участием степеней  $a, b, c$  и  $d$ . Таким образом, процесс перехода от одного состояния машины к другому будет состоять из следующих частей: сначала преобразовываем степень  $a$  в степень  $c$ , и степень  $b$  в степень  $d$ , меняем состояние головки  $Q_i$ , вычисляем новый цвет текущей ячейки  $P_j$ , затем переводим степени  $b$  и  $d$  в степени  $a$  и  $c$ .

Состояния машины мы будем моделировать словами  $La^kb^nQ_iP_jM_\varphi H_\alpha R$ . Четверки чисел  $(i, j, k, n)$  достаточно для описания полного состояния машины со всей лентой. При переходе от одного состояния машины к другому, необходимо реализовать определенный вычислительный процесс:

- Если  $(i, j)$  – левая пара, нужно поделить  $k$  (степень буквы  $a$ ) на 4 с остатком  $r$ . Этот остаток есть цвет клетки слева от головки и он будет соответствовать новому значению  $P_j$ . Если же  $(i, j)$  – правая пара, нужно делить  $n$ , в этом случае нам нужен цвет клетки справа от головки. Деление производится с помощью преобразования  $a^k \rightarrow c^{[\frac{k}{4}]}$  (или  $b^n \rightarrow d^{[\frac{n}{4}]}).$

- Умножить  $n$  (или соответственно  $k$ ) на 4 (так мы реализуем сдвиг клеток) и добавить к этому  $t(i, j)$  – новый цвет перекрасившейся текущей

ячейки. Умножение производится с помощью преобразования  $b^n \rightarrow d^{4n}$  (или  $a^k \rightarrow c^{4k}$ );

3. Заменить  $Q_i$  на  $Q_{q(i,j)}$  (в соответствии с инструкцией для  $(i,j)$ );
4. Заменить  $P_i$  на остаток из пункта 1;
5. Заменить  $M_\varphi$  на  $M_0$  или  $M_1$ , в соответствии с ориентацией новой пары  $(i,j)$ .
6. Восстановить новые значения степеней  $a$  и  $b$ :  $c^k \rightarrow a^k$ ,  $d^n \rightarrow b^n$ .

Таким образом, весь процесс перехода от одного состояния к другому можно разбить на три этапа: преобразование степени  $a$  в степень  $c$ , преобразование степени  $b$  в степень  $d$ , и восстановление новых значений степеней  $a$  и  $b$  по степеням  $c$  и  $d$ .

Для того, чтобы контролировать, какой этап реализуется, будем использовать дополнительный флаг – бит информации: в слове будет буква  $H_\alpha$ , где  $0 \leq \alpha \leq 2$ . Эта буква служит индикатором, какая часть процесса в настоящее время реализуется.  $H_0$  означает, что в данный момент степень  $b$  преобразуется в степень  $d$ ,  $H_1$  означает, что в данный момент степень  $a$  преобразуется в степень  $c$ ,  $H_2$  означает, что идет обратный процесс: степени  $c$  и  $d$  преобразуются в степени  $a$  и  $b$ . Все операции будем проводить с помощью слов вида:  $La^k b^n Q_i P_j M_\varphi H_\alpha c^m d^l R$ , где  $0 \leq \alpha \leq 2$ . Таким образом, фактически реализуется машина Минского с 4 лентами.

В построении особую роль будет играть буквы  $t$  и  $s$ . Каждое определяющее соотношение будет иметь одну из следующих форм:

$$tAB = AtB, \text{ где под слова } A, B \text{ не содержат } t;$$

$$sA = As, \text{ где под слово } A \text{ не содержит } s;$$

$$tA = Bs, \text{ где под слова } A, B \text{ не содержат } t \text{ и } s.$$

То есть, умножение на  $t$  слева играет роль “элементарной операции” и вызывает преобразования над словом  $La^k b^n Q_i P_j M_\varphi H_\alpha c^m d^l R$ :  $t$  с помощью соотношений  $tAB = AtB$  “продвигается” в слове, затем, с помощью  $tA = Bs$ , происходит преобразование слова в соответствии с вычислительным процессом, указанным выше. Таким образом, с помощью нескольких умножений на  $t$  реализуется переход от одного состояния машины Тьюринга в другое.

Переход от одного полного состояния  $(i_1, j_1, k_1, n_1)$  к другому  $(i_2, j_2, k_2, n_2)$  соответствует цепочке эквивалентных переходов от слова  $La^{k_1} b^{n_1} Q_{i_1} M_{\varphi(i_1, j_1)} P_{j_1} H_0 R$  к слову  $La^{k_2} b^{n_2} Q_{i_2} M_{\varphi(i_2, j_2)} P_{j_2} H_0 R$ . Мы вводим определяющие соотношения таким образом, что переход осуществляется за счет нескольких умножений на  $t$ , то есть, существует такое натураль-

ное  $N$ , что

$$t^N La^{k_1} b^{n_1} Q_{i_1} P_{j_1} M_{\varphi(i_1, j_1)} H_0 R \equiv a^{k_2} b^{n_2} Q_{i_2} P_{j_2} M_{\varphi(i_2, j_2)} H_0 R s^N$$

## 1.2 Универсальная машина Тьюринга и определяющие соотношения

Универсальная машина Тьюринга, построенная Минским, задается следующими инструкциями:

$$\begin{aligned} (0, 0) &\rightarrow (L, 4, 1) (0, 1) \rightarrow (L, 1, 3) (0, 2) \rightarrow (R, 0, 0) (0, 3) \rightarrow (R, 0, 1) \\ (1, 0) &\rightarrow (L, 1, 2) (1, 1) \rightarrow (L, 1, 3) (1, 2) \rightarrow (R, 0, 0) (1, 3) \rightarrow (L, 1, 3) \\ (2, 0) &\rightarrow (R, 2, 2) (2, 1) \rightarrow (R, 2, 1) (2, 2) \rightarrow (R, 2, 0) (2, 3) \rightarrow (L, 4, 1) \\ (3, 0) &\rightarrow (R, 3, 2) (3, 1) \rightarrow (R, 3, 1) (3, 2) \rightarrow (R, 3, 0) (3, 3) \rightarrow (L, 4, 0) \\ (4, 0) &\rightarrow (L, 5, 2) (4, 1) \rightarrow (L, 4, 1) (4, 2) \rightarrow (L, 4, 0) (4, 3) \rightarrow \text{СТОП} \\ (5, 0) &\rightarrow (L, 5, 2) (5, 1) \rightarrow (L, 5, 1) (5, 2) \rightarrow (L, 6, 2) (5, 3) \rightarrow (R, 2, 1) \\ (6, 0) &\rightarrow (R, 0, 3) (6, 1) \rightarrow (R, 6, 3) (6, 2) \rightarrow (R, 6, 2) (6, 3) \rightarrow (R, 3, 1) \end{aligned}$$

В полу группе  $G$  будем использовать следующий алфавит:

$$\{t, s, L a, b, Q_0 \dots Q_6, P_0 \dots P_3, M_0, M_1, H_0, H_1, H_2, c, d, R, \}$$

Для всех пар, кроме  $(4, 3)$  определены функции  $q(i, j)$  – новое состояние после выполнения инструкции,  $t(i, j)$  – цвет, который принимает текущая клетка (головка уходит из нее после выполнения инструкции),  $\varphi(i, j)$  – ориентация пары  $(i, j)$ , то есть  $\varphi(i, j) = 0$ , если  $(i, j)$  – левая пара или пара  $(4, 3)$  и  $\varphi(i, j) = 1$ , если  $(i, j)$  – правая пара.

Введем следующие соотношения:

$$tLa = Lta; \quad (1.1)$$

$$tLb = Ltb; \quad (1.2)$$

$$tLQ_i = LtQ_i; \quad \text{где } 0 \leq i \leq 6 \quad (1.3)$$

$$ta^5 = ata^4, \quad (1.4)$$

$$ta^r b = a^r tb, \quad \text{где } 1 \leq r \leq 4 \quad (1.5)$$

$$tb^5 = btb^4 \quad (1.6)$$

$$tb^4 Q_i P_j M_0 H_0 = Q_i P_j M_0 H_0 ds, \quad (1.7)$$

$$tb^r Q_i P_j M_0 H_0 = Q_{q(i,j)} P_r M_0 H_1 s, \quad 1 \leq r \leq 3 \quad (1.8)$$

$$ta^r Q_i P_j M_0 H_0 = a^r Q_{q(i,j)} P_0 M_0 H_1 s, \quad 0 \leq r \leq 4 \quad (1.9)$$

$$ta^4 Q_i P_j M_0 H_1 = Q_i P_j M_0 H_1 c^{16} s, \quad (1.10)$$

$$ta^r Q_i P_j M_0 H_1 = Q_i P_j M_{\varphi(i,j)} H_2 c^{4r+t(i,j)} s, \quad 0 \leq r \leq 3 \quad (1.11)$$

$$tb^4 Q_i P_j M_1 H_0 = Q_i P_j M_1 H_0 d^{16} s, \quad (1.12)$$

$$tb^r Q_i P_j M_1 H_0 = Q_i P_j M_1 H_1 d^{4r+t(i,j)} s, \quad 1 \leq r \leq 3 \quad (1.13)$$

$$ta^r Q_i P_j M_1 H_0 = a^r Q_i P_j H_1 M_1 d^{t(i,j)} s, \quad 0 \leq r \leq 4 \quad (1.14)$$

$$ta^4 Q_i P_j M_1 H_1 = Q_i P_j M_1 H_1 c s, \quad (1.15)$$

$$ta^r Q_i P_j M_1 H_1 = Q_{q(i,j)} P_r M_{\varphi(i,j)} H_2 s, \quad 0 \leq r \leq 3 \quad (1.16)$$

$$sc = cs \quad (1.17)$$

$$sd = ds \quad (1.18)$$

$$sR = Rs \quad (1.19)$$

$$ta^r Q_i P_j M_{\varphi} H_2 c = a^{r+1} Q_i P_j M_{\varphi} H_2 s, \quad \text{где } \varphi = 0, 1, \text{и } 0 \leq r \leq 4 \quad (1.20)$$

$$ta^r Q_i P_j M_{\varphi} H_2 R = a^r Q_i P_j M_{\varphi} H_0 R s, \quad \text{где } \varphi = 0, 1, \text{и } 1 \leq r \leq 4 \quad (1.21)$$

$$ta^r Q_i P_j M_{\varphi} H_2 d = a^r b Q_i P_j M_{\varphi} H_2 s, \quad \text{где } \varphi = 0, 1, \text{и } 1 \leq r \leq 4 \quad (1.22)$$

$$tb^r Q_i P_j M_{\varphi} H_2 d = b^{r+1} Q_i P_j M_{\varphi} H_2 s, \quad \text{где } \varphi = 0, 1, \text{и } 0 \leq r \leq 4 \quad (1.23)$$

$$tb^r Q_i P_j M_{\varphi} H_2 R = b^r Q_i P_j M_{\varphi} H_0 R s, \quad \text{где } \varphi = 0, 1, \text{и } 0 \leq r \leq 4 \quad (1.24)$$

$$Q_4 P_3 = 0. \quad (1.25)$$

**Примечание.** В случае, если в соотношении встречаются параметры, оно выписывается для всех указанных значений параметра. В случае, если фигурирует пара  $(i, j)$  – считается, что это любая пара, кроме  $(4, 3)$ .

Пусть имеется слово  $t^N La^k b^n Q_i P_j M_{\varphi} H_0 R$ , соответствующее какому-то состоянию описанной машины. Как введенные соотношения помогают нам перейти к следующему состоянию?

Соотношения (1.1)–(1.6) служат для того, чтобы можно было провести  $t$  с левого края до букв  $Q_i$ ,  $P_j$ , реализующих головку машины. Соотношения (1.17)–(1.21) служат для выведения  $s$  на правый край слова. Соотношения (1.7)–(1.16) и (1.20)–(1.24) непосредственно моделируют вычислительный процесс, указанный в плане построения:

1. Если  $(i, j)$  - левая пара, поделить  $k$  (степень буквы  $a$ ) на 4 с остатком  $r$ . – соотношения (1.15),(1.16). Если же  $(i, j)$  - правая пара, нужно аналогично делить  $n$  – соотношения (1.7),(1.8);
2. Умножить  $n$  (или соответственно  $k$ ) на 4 (так мы реализуем сдвиг клеток) и добавить к этому  $t(i, j)$  – новый цвет перекрасившейся текущей ячейки. Умножение производится с помощью преобразования  $b^n \rightarrow d^{4n}$  (или  $a^k \rightarrow c^{4k}$ ) – соотношения (1.12),(1.13) (для  $n$ ) и (1.10),(1.11) (для  $k$ );
3. Заменить  $Q_i$  на  $Q_{q(i,j)}$  (в соответствии с инструкцией для  $(i, j)$ ) – соотношения (1.8) и (1.16);
4. Заменить  $P_i$  на остаток из пункта 1 – соотношения (1.8) и (1.16);
5. Заменить  $M_\varphi$  на  $M_0$  или  $M_1$ , в соответствии с ориентацией новой пары  $(i, j)$ . – соотношения (1.11) и (1.16);
6. Восстановить новые значения степеней  $a$  и  $b$ :  $k \rightarrow a^k$ ,  $d^n \rightarrow b^n$  – соотношения (1.20) – (1.24).

Кроме того, соотношение (1.25) реализует остановку машины.

### 1.3 Делители нуля и остановка машины

Ясно, что полное состояние машины (вместе с лентой) описывается четырьмя числами: состоянием головки  $i$ , цветом текущей клетки  $j$ , числом  $k$ , кодирующим состояние клеток слева от головки и числом  $n$ , кодирующим состояние клеток справа от головки. Будем обозначать полное состояние машины как  $M(i, j, k, n)$ .

**Определение 1.3.1.** Будем считать, что полное состояние машины характеризуется четверкой  $(i, j, k, n)$ , если, в данный момент: состояние головки  $i$ , цвет текущей клетки  $j$ ,  $k = \sum_{f=0}^{\infty} a_f 4^f$ ,  $n = \sum_{f=0}^{\infty} b_f 4^f$ , где  $a_f$  – цвета клеток, перечисленные от головки налево,  $b_f$  – цвета клеток, перечисленные от головки направо. Очевидно, что в обоих суммах всегда существует конечное число ненулевых слагаемых, так как количество непустых ячеек всегда конечно.

Каждое полное состояние однозначно определяет следующее полное состояние и так далее. Будем говорить, что машина переходит из состо-

яния  $M(i_1, j_1, k_1, n_1)$  в состояние  $M(i_2, j_2, k_2, n_2)$ , если машина, начиная работу в состоянии  $M(i_1, j_1, k_1, n_1)$  за несколько шагов переходит в состояние  $M(i_2, j_2, k_2, n_2)$ .

Нашей основной целью будет доказательство следующей теоремы:

**Теорема 1.3.1.** *Пусть машина Тьюринга, описанная выше, начинает работу в состоянии  $M(i, j, k, n)$ . Обозначим  $\varphi = 0$ , если  $(i, j)$  – левая пара или пара  $(4, 3)$  и  $\varphi(i, j) = 1$ , если  $(i, j)$  – правая пара.*

*Машина останавливается тогда и только тогда, когда слово  $La^k b^n Q_i P_j M_\varphi H_0 R$  является делителем нуля в алгебре с определяющими соотношениями (1.1)–(1.25).*

Сначала докажем несколько предложений.

**Предложение 1.3.1.** *Пусть  $n, k$  – натуральные числа. В полугруппе  $G$  справедливы следующие эквивалентности:*

1.  $tLa^k b^n \equiv La^{k-4} tb^4$ , если  $n \geq 5$ ;
2.  $tLa^k b^n \equiv La^k tb^n$ , если  $n \leq 4$ ;

*Доказательство.* Допустим сначала, что  $k \geq 5$ . Тогда применяя  $tLa = Lta$  и несколько раз  $ta^5 = ata^4$  – соотношения (1.1) и (1.4), мы приводим слово  $tLa^k b^n$  к виду  $La^{k-4} ta^4 b$ . Далее, применяем  $ta^4 b = ata^3 b$ ,  $ta^3 b = ata^2 b$ ,  $ta^2 b = atab$ ,  $tab = atb$  – соотношение (1.5) (при разных  $r$ ), и получаем  $La^k tb^n$ . Если  $n \leq 4$ , то на этом останавливаемся (и пункт 2 доказан). Если  $n \geq 5$ , то соответствия пункту 1 мы добиваемся, применив несколько раз  $tb^5 = btb^4$  – соотношение (1.6).

Если  $1 \leq k \leq 4$ , мы действуем аналогично, но в этом случае соотношение  $ta^5 = ata^4$  мы не применяем, пропуская этот этап.  $\square$

**Предложение 1.3.2.** *Пусть  $k, n$  – неотрицательные целые числа, не равные нулю одновременно,  $0 \leq t(i, j) \leq 3$  – цвет, который принимает текущая клетка после выполнения инструкции  $(i, j)$ ,  $0 \leq q(i, j) \leq 6$  – состояние головки после выполнения инструкции  $(i, j)$ .*

*Тогда, если  $(i, j)$  – правая пара, имеет место следующая эквивалентность:*

$$t^N La^k b^n Q_i P_j M_1 H_0 R \equiv L Q_{q(i,j)} P_r M_{\varphi(q,r)} H_2 c^{4k+t(i,j)} d^{[n]} R s^N,$$

*где  $\varphi(q, r) = 0$  или  $1$  – в зависимости от того, левая пара  $(q, r)$  или правая,  $[x]$  – наибольшее целое, не превосходящее  $x$ ,  $r$  – остаток от деления  $n$  на  $4$ , и  $N = [\frac{k}{4}] + [\frac{n}{4}] + 2$ .*

Если же  $(i, j)$  – левая пара, имеет место следующая эквивалентность:

$$t^N La^k b^n Q_i P_j M_0 H_0 R \equiv L Q_{q(i,j)} P_r M_{\varphi(q,r)} H_2 c^{[\frac{k}{4}]} d^{4n+t(i,j)} R s^N,$$

где  $\varphi(q, r) = 0$  или  $1$  – в зависимости от того, левая пара  $(q, r)$  или правая, где  $[x]$  – наибольшее целое, не превосходящее  $x$ ,  $r$  – остаток от деления  $k$  на  $4$ , и  $N = [\frac{k}{4}] + [\frac{n}{4}] + 2$ .

*Доказательство.* Докажем сначала промежуточные эквивалентности:

$$t^{[\frac{n}{4}]+1} La^k b^n Q_i P_j M_1 H_0 R \equiv La^k Q_{q(i,j)} P_r M_1 H_1 d^{[\frac{n}{4}]} R s^{[\frac{n}{4}]+1}, \text{ где } r = n - 4[\frac{n}{4}]$$

– остаток при делении  $n$  на  $4$ , для правого случая, и

$$t^{[\frac{n}{4}]+1} La^k b^n Q_i P_j M_0 H_0 R \equiv La^k Q_i P_j M_0 H_1 d^{4n+t(i,j)} R s^{[\frac{n}{4}]+1} \text{ – для левого случая.}$$

Рассмотрим слово  $t^N La^k b^n Q_i P_j M_\varphi H_0 R$ , где  $\varphi$  соответствует ориентации пары  $(i, j)$ . Возможны три случая:  $n = 0$ ,  $1 \leq n \leq 3$  и  $n \geq 4$ .

Если  $n = 0$ , нам надо доказать

$$t La^k Q_i P_j M_1 H_0 R \equiv La^k Q_{q(i,j)} M_1 P_0 H_1 R s, \text{ для правого случая, и}$$

$$t La^k Q_i P_j M_0 H_0 R \equiv La^k Q_i P_j M_0 H_1 d^{t(i,j)} R s, \text{ для левого случая.}$$

Для этого применим  $t La = Lta$  – соотношение (1.1). Получим слово  $Lta^k Q_i P_j M_\varphi H_0 R$ . Если  $k \leq 4$ , тогда в правом случае применим  $ta^r Q_i P_j M_1 H_0 \equiv a^r Q_{q(i,j)} P_0 M_1 H_1 s$  – соотношение (1.9), а в левом случае –  $ta^r Q_i P_j M_0 H_0 \equiv a^r Q_i P_j M_0 H_1 d^{t(i,j)} s$  – соотношение (1.14). С учетом  $sR = Rs$ , получаем то, что требуется. Если же  $k \geq 5$ , несколько раз применим  $ta^5 = ata^4$  – соотношение (1.4), получаем слово  $La^{k-4} ta^4 Q_i P_j M_\varphi H_0 R$ . Теперь применяем соотношения (1.9), (1.14) (для  $r = 4$ ) и  $sR = Rs$ , как в случае  $k \leq 4$ .

Если  $n \leq 3$ , тогда  $N = 1$ . Применяя вторую часть ( $t La^k b^n \equiv La^k tb^n$ ) предложения (1.3.1), получаем  $La^k tb^n Q_i P_j M_\varphi H_0 R$ . Теперь используем:

для правого случая –  $tb^r Q_i P_j M_1 H_0 = Q_{q(i,j)} P_r M_1 H_1 s$  – соотношение (1.8) и получаем  $La^k Q_{q(i,j)} P_r M_1 H_1 s R$ , где  $r = n$ ;

для левого случая –  $tb^r Q_i P_j M_0 H_0 = Q_i P_j M_0 H_1 d^{4r+t(i,j)} s$  – соотношение (1.13) и получаем  $La^k Q_i P_j M_0 H_1 d^{4n+t(i,j)} s R$ .

Теперь применяя  $sR = Rs$  – соотношение (1.19) в обоих случаях приводим оба слова к требуемому виду.

Если  $n \geq 4$ , применяем вторую часть ( $t La^k b^n \equiv La^k b^{n-4} tb^4$ ) предложения (1.3.1), получаем  $La^k b^{n-4} tb^4 Q_i P_j M_\varphi H_0 R$ . Теперь используем:

для правого случая –  $tb^4 Q_i P_j M_1 H_0 = Q_i P_j M_1 H_0 ds$  – соотношение (1.7) и получаем  $t^{N-1} La^k b^{n-4} Q_i P_j M_1 H_0 ds R$ , где  $r = n$ ;

для левого случая –  $tb^4Q_iP_jM_0H_0 = Q_iP_jM_0H_0d^{16}s$  – соотношение (1.12) и получаем  $t^{N-1}La^k b^{n-4}Q_iP_jM_0H_0d^{16}sR$ .

Теперь используем  $sR = Rs$  в обоих случаях. Повторяя последние операции (предложение (1.3.1), соотношение  $tb^4Q_iP_jM_1H_0 = Q_iP_jH_0ds$  в правом случае и соотношение  $tb^4Q_iP_jH_0 = Q_iP_jM_1H_0d^{16}s$  в левом случае) а также используя  $sd = ds$  и  $sR = Rs$  – соотношения (1.18) и (1.19), мы приводим слова к видам:

$$tLa^k b^r Q_iP_jM_1H_0d^{[\frac{n}{4}]}Rs^{[\frac{n}{4}]}, \text{ где } r < 4, r \equiv n \pmod{4} \text{ – в правом случае;}$$

$$tLa^k b^r Q_iP_jM_0H_0d^{4[\frac{n}{4}]}Rs^{[\frac{n}{4}]}, \text{ где } r < 4, r \equiv n \pmod{4} \text{ – в левом случае;}$$

Теперь действуем как в случае  $n \leq 3$ : применяем предложение (1.3.1) и соотношение  $tb^r Q_iP_jM_1H_0 = Q_{q(i,j)}P_rH_1s$  для правого случая и соотношение  $tb^r Q_iP_jH_0 = Q_iP_jM_0H_1d^{4r+t(i,j)}s$  для левого случая. С учетом  $sd = ds$ ,  $sR = Rs$  получаем слова:

$La^k Q_{q(i,j)}P_rM_1H_1d^{\frac{n}{4}}Rs^{[\frac{n}{4}]+1}$ , где  $r = n - 4[\frac{n}{4}]$  – остаток при делении  $n$  на 4, для правого случая, и

$$La^k Q_iP_jM_0H_1d^{4n+t(i,j)}Rs^{\frac{n}{4}+1} \text{ – для левого случая.}$$

**Примечание.** Заметим, что в правом случае уже произошла замена пары  $Q_iP_j$  на пару  $Q_{q(i,j)}P_r$ , и при этом могла сменится ориентация пары. Фиксировать ту ориентацию, что была в начале (правую), нам помогает буква  $M_1$ .

Таким образом, мы доказали промежуточные эквивалентности. Теперь мы докажем, что

для правого случая:  $t^{[\frac{k}{4}]+1}La^k Q_iP_jM_1H_1R \equiv LQ_iP_jM_{\varphi(i,j)}H_2^{4k+t(i,j)}s^{[\frac{k}{4}]+1}$ ,

где  $\varphi(i, j) = 0$  или 1 в зависимости от ориентации пары  $(i, j)$ ;

для левого случая:  $t^{[\frac{k}{4}]+1}La^k Q_iP_jM_0H_1R \equiv La^k Q_{q(i,j)}P_rM_{\varphi(q,r)}H_2c^{[\frac{k}{4}]}s^{[\frac{k}{4}]+1}$ ,

где  $r \equiv k \pmod{4}$ , и  $\varphi(i, j) = 0$  или 1 в зависимости от ориентации пары  $(i, j)$ .

Возможны три случая:  $k = 0$ ,  $1 \leq k \leq 3$  и  $k \geq 4$ .

Если  $k = 0$ , применяя  $tLQ_i = LtQ_i$  – соотношение (1.3) получаем слово  $LtQ_iP_jH_1$ . Теперь в правом случае применим (для  $r = 0$ )  $ta^r Q_iP_jM_1H_1 \equiv Q_iP_jM_{\varphi(i,j)}H_2c^{4r+t(i,j)}s$ , где  $\varphi(i, j)$  соответствует ориентации пары  $(i, j)$  – соотношение (1.11), а в левом случае (тоже для  $r = 0$ )  $-ta^r Q_iP_jM_0H_1 \equiv Q_{q(i,j)}P_rM_{\varphi(q,r)}H_2s$ , где  $\varphi(q, r)$  соответствует ориентации пары  $(q, r)$  – соотношение (1.16). С учетом  $sR = Rs$ , получаем то, что требуется.

Если  $1 \leq k \leq 3$ , применяя  $tLa = Lta$  – соотношение (1.1) получаем слово  $Lta^k Q_iP_jH_1$ . Теперь в правом случае применим (для  $r = k$ )  $ta^r Q_iP_jM_1H_1 \equiv Q_iP_jM_{\varphi(i,j)}H_2c^{4r+t(i,j)}s$  – соотношение (1.11), а в левом

случае (тоже для  $r = k$ ) –  $ta^r Q_i P_j M_0 H_1 \equiv Q_{q(i,j)} P_r M_{\varphi(i,j)} H_2 s$  – соотношение (1.16). С учетом  $sR = Rs$ , получаем то, что требуется.

Если  $k \geq 4$ , применяя  $tLa = Lta$  – соотношение (1.1) и несколько раз  $ta^5 = ata^4$  – соотношение (1.4), получаем слово  $t^{[\frac{k}{4}]} La^{k-4} ta^4 Q_i P_j M_\varphi H_1$ . Теперь используем: в правом случае  $ta^4 Q_i P_j M_1 H_1 \equiv Q_i P_j M_1 H_1 c^{16} s$  – соотношение (1.10), в левом случае  $ta^4 Q_i P_j M_0 H_1 \equiv Q_i P_j M_0 H_1 c s$  – соотношение (1.15), и получим:

в правом случае:  $t^{[\frac{k}{4}]} La^{k-4} Q_i P_j M_1 H_1 c^{16} s$ ;

в левом случае:  $t^{[\frac{k}{4}]} La^{k-4} Q_i P_j M_0 H_1 c s$ .

К слову  $t^{[\frac{k}{4}]} La^{k-4} Q_i P_j M_\varphi H_1$ , где  $\varphi = 0$  или  $1$ , можно применить индукционное предположение ( $k$  уменьшилось на  $4$ ). С учетом  $sc = cs$  и  $sR = Rs$  – соотношения (1.17) и (1.19), получаем то, что требуется.

Теперь докажем утверждение предложения. Рассмотрим слово  $t^N La^k b^n Q_i P_j M_\varphi H_0 R$ , где  $\varphi = 0$  или  $1$ , и  $N = [\frac{k}{4}] + [\frac{n}{4}] + 2$ . Применяя первую промежуточную эквивалентность, получаем:

в правом случае:  $t^{[\frac{k}{4}]+1} La^k Q_{q(i,j)} P_r M_1 H_1 d^{[\frac{n}{4}]} R s^{[\frac{n}{4}]+1}$ , где  $r = n - 4[\frac{n}{4}]$  – остаток при делении  $n$  на  $4$ ;

в левом случае:  $t^{[\frac{k}{4}]+1} La^k Q_i P_j M_0 H_1 d^{4n+t(i,j)} R s^{[\frac{n}{4}]+1}$ .

Теперь в обоих случаях применим вторые промежуточные эквивалентности:

для правого случая:  $t^{[\frac{k}{4}]+1} La^k Q_i P_j M_1 H_1 \equiv L Q_i P_j M_{\varphi(i,j)} H_2^{4k+t(i,j)} s^{[\frac{k}{4}]+1}$ ,

где  $\varphi(i,j) = 0$  или  $1$  в зависимости от ориентации пары  $(i,j)$ ;

для левого случая:  $t^{[\frac{k}{4}]+1} La^k Q_i P_j M_0 H_1 \equiv L Q_{q(i,j)} P_r M_{\varphi(q,r)} H_2 c^{[\frac{k}{4}]} s^{[\frac{k}{4}]+1}$ ,

где  $r \equiv k \pmod{4}$ , и  $\varphi(i,j) = 0$  или  $1$  в зависимости от ориентации пары  $(i,j)$ .

Получаем:

в правом случае:

$$L Q_{q(i,j)} P_r M_{\varphi(i,j)} H_2^{4k+t(i,j)} s^{[\frac{k}{4}]+1} d^{[\frac{n}{4}]} R s^{[\frac{n}{4}]+1},$$

где  $r = n - 4[\frac{n}{4}]$  – остаток при делении  $n$  на  $4$ ;

в левом случае:

$$L Q_{q(i,j)} P_r M_{\varphi(q,r)} H_2 c^{[\frac{k}{4}]} s^{[\frac{k}{4}]+1} d^{4n+t(i,j)} R s^{[\frac{n}{4}]+1}.$$

Применив  $sd = ds$ ,  $sc = cs$  и  $sR = Rs$ , получаем, что требуется в условии предложения.  $\square$

**Предложение 1.3.3.** Пусть  $\varphi = 0$  или  $1$ . Справедлива следующая эквивалентность:

$$t^{n+k+1}LQ_iP_jM_\varphi H_2c^kd^nR \equiv La^kb^nQ_iP_jM_\varphi H_0Rs^{n+k+1};$$

*Доказательство.* Докажем сначала следующие эквивалентности:

$$1. tLa^mQ_iP_jM_\varphi H_2c \equiv La^{m+1}P_jQ_iM_\varphi H_2s.$$

$$2. tLa^mb^lQ_iP_jM_\varphi H_2d \equiv La^kb^{l+1}P_jQ_iM_\varphi H_2s.$$

1. Если  $m = 0$ , то достаточно применить  $tLQ_i = LtQ_i$  и  $ta^rQ_iP_jM_\varphi H_2c = a^{r+1}Q_iP_jM_\varphi H_2s$  (для  $r = 0$ ) – соотношения (1.3) и (1.20). Если  $1 \leq m \leq 4$ , применяем  $tLa = Lta$  и  $ta^rQ_iP_jM_\varphi H_2c = a^{r+1}Q_iP_jM_\varphi H_2s$  (для  $r = m$ ) – соотношения (1.1) и (1.20). В случае  $m \geq 5$ , применяем  $tLa = Lta$ , затем несколько раз  $ta^5 = ata^4$  – соотношение (1.4), и все сводится опять к применению соотношения (1.20).

2. Если  $l = 0$ , то действуем аналогично пункту 1, только вместо соотношения (1.20) применяем  $ta^rQ_iP_jM_\varphi H_2d = a^rbQ_iP_jM_\varphi H_2s$  – соотношение (1.22).

Если  $1 \leq l \leq 4$ , применяя предложение (1.3.1), получаем слово  $La^mtb^lQ_iP_jM_\varphi H_2d$ . Теперь используя  $tb^rQ_iP_jM_\varphi H_2d = b^{r+1}Q_iP_jM_\varphi H_2s$  (для  $r = l$ ) – соотношение (1.23), получаем, что требуется.

Если  $l \geq 5$ , используя предложение (1.3.1), получаем слово  $La^mb^{l-4}tb^4Q_iP_jM_\varphi H_2d$ . Опять применяя соотношение (1.23) (для  $r = 4$ ), получаем, что требуется.

Теперь докажем утверждение предложения. Рассмотрим слово  $t^{n+k+1}LQ_iP_jM_\varphi H_2c^kd^nR$ .

Пусть сначала  $n = 0$ . Если  $k = 0$ , то применяя  $tb^rQ_iP_jM_\varphi H_2R = b^rQ_iP_jM_\varphi H_0Rs$  – соотношение (1.24) для  $r = 0$ , получаем, что требуется. Пусть  $k \geq 1$ . Применяя к слову  $t^{k+1}LQ_iP_jM_\varphi H_2c^kd^nR$  несколько раз первую доказанную эквивалентность для  $m = 0, \dots, k - 1$ , попутно используя  $sc = cs$  и  $sR = Rs$  получим  $tLa^kQ_iP_jM_\varphi H_2R$ . Теперь применим  $tLa = Lta$ , и несколько раз  $ta^5 = ata^4$  – соотношения (1.1) и (1.4). В получившемся слове  $La^{k-4}ta^4Q_iP_jM_\varphi H_2R$  достаточно применить  $ta^rQ_iP_jM_\varphi H_2R = a^rQ_iP_jM_\varphi H_0Rs$  – соотношение (1.21), (для  $r = 4$ ) и мы получаем то, что требуется.

Пусть  $n \geq 1$ . Рассмотрим слово  $t^{n+k+1}LQ_iP_jM_\varphi H_2c^kd^nR$ . Используя несколько раз первую доказанную эквивалентность для  $m = 0, \dots, k - 1$ , попутно учитывая  $sc = cs$ ,  $sd = ds$ ,  $sR = Rs$  получим  $t^{n+1}La^kQ_iP_jM_\varphi H_2d^nRs^k$ . Теперь несколько раз применим вторую доказанную эквивалентность для  $l = 0, \dots, n - 1$ , попутно используя  $sd = ds$

и  $sR = Rs$ . Получаем  $tLa^k b^n Q_i P_j M_\varphi H_2 R s^{n+k}$ . Теперь применяя предложение (1.3.1) и  $tb^r Q_i P_j M_\varphi H_2 R = b^r Q_i P_j M_\varphi H_0 R s$  – соотношение (1.24) окончательно получаем требуемую эквивалентность.  $\square$

**Предложение 1.3.4.** *Рассмотрим один шаг работы описанной выше машины. Пусть, ее текущее состояние  $M(i, j, k, n)$ , а следующее –  $M(\hat{i}, \hat{j}, \hat{k}, \hat{n})$ . Пусть также,  $\varphi$  соответствует ориентации пары  $(i, j)$ , то есть  $\varphi = 0$ , если пара левая и  $\varphi = 1$ , если пара правая, и  $\hat{\varphi}$  соответствует ориентации пары  $(\hat{i}, \hat{j})$ .*

Тогда существует такое натуральное  $N$ , что

$$t^N La^k b^n Q_i P_j M_\varphi H_0 R \equiv La^{\hat{k}} b^{\hat{n}} Q_{\hat{i}} P_{\hat{j}} M_{\hat{\varphi}} H_0 R s^N.$$

*Доказательство.* Рассмотрим слово  $La^k b^n Q_i P_j M_\varphi H_0 R$ . Допустим,  $(i, j)$  – правая пара. Тогда  $\varphi = 1$ . Используя предложение (1.3.2), находим такое  $N_1$ , что

$$t^{N_1} La^k b^n Q_i P_j M_\varphi H_0 R \equiv LQ_{q(i,j)} P_r M_{\varphi(q,r)} H_2 c^{4k_1+t(i,j)} d^{[\frac{n}{4}]} R s^{N_1},$$

где  $r$  – остаток от деления  $n_1$  на 4,  $\varphi(q, r) = 0$  или 1 – в зависимости от того, левая пара  $(q, r)$  или правая. Теперь к слову  $LQ_{q(i,j)} P_r M_{\varphi(q,r)} H_2 c^{4k+t(i,j)} d^{[\frac{n}{4}]} R$  применим предложение (1.3.3) и найдем такое  $N_2$ , что

$$t^{N_2} LQ_{q(i,j)} P_r M_{\varphi(q,r)} H_2 c^{4k+t(i,j)} d^{[\frac{n}{4}]} R \equiv La^{4k+t(i,j)} b^{[\frac{n}{4}]} Q_{q(i,j)} P_r M_{\varphi(q,r)} H_0 R s^{N_2}.$$

Таким образом, имеет место эквивалентность:

$$t^{N_1+N_2} La^k b^n Q_i P_j M_1 H_0 R \equiv La^{4k+t(i,j)} b^{[\frac{n}{4}]} Q_{q(i,j)} P_r M_{\varphi(q,r)} H_0 R s^{N_1+N_2}.$$

Так как  $(i, j)$  – правая пара, и  $t(i, j)$  – новый цвет ячейки, из которой головка уходит, новое значение  $\hat{k}$  будет равно  $4k + t(i, j)$ . Цвет новой текущей ячейки мы находим как остаток от деления  $n$  на 4. А новое значение  $\hat{n}$  есть целочисленный результат этого деления:  $\hat{n} = [\frac{n}{4}]$ . Таким образом, мы получили требуемую эквивалентность.

Случай, когда  $(i, j)$  – левая пара, рассматривается аналогично.  $\square$

**Предложение 1.3.5.** *Перенесем в левую часть все слова в каждом из соотношений (1.1)–(1.25). Левые части получившихся равенств образуют базис Грёбнера в порождаемом ими идеале, относительно лексикографического порядка, соответствующего порядку букв*

$$\{t, s, La, b, Q_0 \dots Q_6, P_0 \dots P_3, M_0, M_1, H_0, H_1, H_2, c, d, R, \}.$$

*Доказательство.* Заметим, что во всех соотношениях в левой части стоит более старший моном. Проверим отсутствие зацеплений среди старших мономов. Все старшие мономы начинаются с букв  $t$  или  $s$ . Кроме того, эти буквы входят только в качестве первых букв мономов. Следовательно, единственной возможностью зацепления является ситуация, когда один моном является началом другого. Легко убедится, что таких мономов нет.  $\square$

Определяющие соотношения естественно рассматривать как редукции – линейные операторы, переводящие моном в левой части соотношения в моном в правой части, а остальные мономы оставляющие на месте. При данных определяющих соотношениях, моном всегда редуцируется либо в моном, либо в нуль.

**Предложение 1.3.6.** *Положим  $\varphi(i, j) = 1$ , если пара  $(i, j)$  – правая, и  $\varphi(i, j) = 0$ , если левая.*

*Следующие утверждения эквивалентны:*

- (i) *Описанная выше машина Тьюринга, начав работу в состоянии  $M(i, j, k, n)$ , через несколько шагов останавливается, то есть приходит в состояние с  $i = 4, j = 3$ .*
- (ii) *Существует такое натуральное  $N$ , что  $t^N La^k b^n Q_i P_j M_\varphi H_0 R \equiv 0$ .*

*Доказательство.* Сначала докажем, что из первого утверждения следует второе. Пусть наша машина Тьюринга, начав работу в состоянии  $M(i, j, k, n)$ , через несколько шагов приходит в состояние с  $i = 4, j = 3$ .

Допустим,  $M(i, j, k, n)$  переходит в  $M(4, 3, \hat{k}, \hat{n})$  за один шаг. Тогда согласно предложению (1.3.4), существует такое  $N$ , что имеет место эквивалентность

$$t^N La^k b^n Q_i P_j M_\varphi H_0 R \equiv La^{\hat{k}} b^{\hat{n}} Q_4 P_3 M_0 H_0 R s^N.$$

Теперь можно применить  $Q_4 P_3 = 0$  – соотношение (1.25) и привести слово к нулю.

Пусть утверждение доказано для переходов с не более чем  $m$  шагами. Пусть наша машина, начав с состояния  $M(i, j, k, n)$  останавливается на  $m + 1$  шагу. Рассмотрим первый переход в этой цепочке. Пусть это переход от  $M(i, j, k, n)$  к  $M(\hat{i}, \hat{j}, \hat{k}, \hat{n})$ . Применяя для этого перехода предложение (1.3.4), получаем, что существует  $N_1$  такое, что

$$t^{N_1} La^k b^n Q_i P_j M_\varphi H_0 R \equiv La^{\hat{k}} b^{\hat{n}} Q_{\hat{i}} P_{\hat{j}} M_{\hat{\varphi}} H_0 R s^{N_1}.$$

К состоянию  $M(\hat{i}, \hat{j}, \hat{k}, \hat{n})$ , применимо предположение индукции. То есть, существует такое  $N_2$ , что  $t^{N_2} La^{\hat{k}} b^{\hat{n}} Q_{\hat{i}} P_{\hat{j}} M_{\hat{\varphi}} H_0 R \equiv 0$ .

Но тогда

$$t^{N_1+N_2} La^k b^n Q_i P_j M_{\varphi} H_0 R \equiv t^{N_2} La^{\hat{k}} b^{\hat{n}} Q_{\hat{i}} P_{\hat{j}} M_{\hat{\varphi}} H_0 R s^{N_1} \equiv 0.$$

Теперь докажем, что из второго утверждения следует первое.

Пусть  $t^N La^k b^n Q_i P_j M_{\varphi} H_0 R \equiv 0$ . Допустим, наша машина, начав с состояния  $M(i, j, k, n)$ , не останавливается. Пусть следующее состояние машины  $M(\hat{i}, \hat{j}, \hat{k}, \hat{n})$ . Согласно предложению (1.3.4), существует такое натуральное  $N_1 \geq 1$ , что

$$t^{N_1} La^k b^n Q_i P_j M_{\varphi} H_0 R \equiv La^{\hat{k}} b^{\hat{n}} Q_{\hat{i}} P_{\hat{j}} M_{\hat{\varphi}} H_0 R s^{N_1}.$$

То есть с помощью степени  $t^{N_1}$  мы перешли к слову, соответствующему следующему состоянию. К этому слову,  $La^{\hat{k}} b^{\hat{n}} Q_{\hat{i}} P_{\hat{j}} M_{\hat{\varphi}} H_0 R$ , можно опять применить предложение (1.3.4) и найти  $N_2 \geq 1$ , для перехода к следующему состоянию. Продолжая аналогичным способом, за конечное число шагов мы получаем  $N_1 + N_2 + \dots + N_x = \hat{N} > N$ . При этом за  $x$  шагов машина переходит в состояние  $M(i_x, j_x, k_x, n_x)$ , причем за все время перехода состояние с  $(i, j) = (4, 3)$  не встретилось, так как это бы означало, что машина останавливается. Значит верна эквивалентность

$$t^{\hat{N}} La^k b^n Q_i P_j M_{\varphi} H_0 R \equiv La^{k_x} b^{n_x} Q_{i_x} P_{j_x} M_{\varphi_x} H_0 R s^{\hat{N}}.$$

Получившееся слово не равно нулю – к нему не применима ни одна редукция. Но нулевое слово  $t^N La^k b^n Q_i P_j M_{\varphi} H_0 R$  является его подсловом. Получили противоречие.  $\square$

Теперь с помощью нескольких предложений докажем, что слово  $La^k b^n Q_i P_j M_{\varphi} H_0 R$  является делителем нуля, только если наша машина, начав с соответствующего состояния, останавливается.

**Предложение 1.3.7.** *Пусть слово  $W$  не приводится к нулю с помощью соотношений (1.1)–(1.25). Тогда для любого натурального  $t$  слова  $Wt^m$  и  $s^m W$  также не приводятся к нулю.*

*Доказательство.* Допустим,  $Wt^m$  приводится к нулю. Заметим, что если в каком либо соотношении используется  $t$ , то справа нее обязательно встречаются другие буквы. Таким образом,  $m$  букв на правом конце слова не могут участвовать ни в одном эквивалентном переходе. Тогда если

$Wt^m$  можно привести к нулю, то и с  $W$  можно было бы сделать то же самое.

Допустим,  $s^m W$  приводится к нулю. Обозначим через  $D$  левое начало слова  $s^m W$ , состоящее из букв  $s, R, d, c$ . Пусть  $DX = s^m W$  – лексикографическое равенство. Тогда  $X$  – подслово  $W$ . Заметим, что соотношения  $sR = Rs, sc = cs, sd = ds$ , не меняют длину и состав букв в слове  $D$ . Остальные соотношения вообще не могут затрагивать слово  $D$ , так их левые и правые части начинаются не с букв  $s, R, d, c$ . То есть каждое соотношение меняет либо слово  $X$ , либо  $D$ . Но тогда если  $s^m W$  можно привести к виду, содержащему  $Q_4 P_3$ , то аналогичное можно проделать со словом  $X$ , а значит и со словом  $W$ .  $\square$

**Предложение 1.3.8.** *Пусть  $A, B$  – ненулевые слова. Тогда если слово вида  $ALa^k b^n Q_i P_j M_\varphi H_0 R B$ , где  $\varphi = \varphi(i, j)$ , приводится к нулю, то существует такое  $N$ , что  $t^N La^k b^n Q_i P_j M_\varphi H_0 R \equiv 0$ .*

*Доказательство.* Обозначим  $a^k b^n Q_i P_j M_\varphi H_0$  как  $U$  и рассмотрим слово  $ALURB$ . Заметим, что все наши соотношения не меняют количества букв  $L$  и  $R$  в слове. Если мы преобразуем слово с помощью соотношения, не содержащего  $L$ , то это преобразование проходит внутри  $A$  или  $URB$ . Если же соотношение затрагивает  $L$ , то это  $tLa = Lta, tLb = Ltb$  или  $tLQ_i = LtQ_i$ . Эти соотношения могут добавить (или убрать)  $t$  к концу слова  $A$ . (“Через  $L$  проходит только  $t$ ”). Аналогично, если соотношение затрагивает  $R$ , то это  $ta^r Q_i P_j M_\varphi H_2 R = a^r Q_i P_j M_\varphi H_0 R s$ , либо  $tb^r Q_i P_j M_\varphi H_2 R = b^r Q_i P_j M_\varphi H_0 R s$ , либо  $sR = R s$ . Эти соотношения могут добавить (или убрать)  $s$  к началу слова  $B$  (“через  $R$  проходит только  $s$ ”). Если,  $ALURB$  приводится к нулю, значит это слово можно привести к виду, содержащему  $Q_4 P_3$ . Это подслово может образоваться либо слева от нашей обозначенной буквы  $L$ , либо между  $L$  и  $R$ , либо справа от  $R$ .

Пусть подслово  $Q_4 P_3$  образовалось слева от  $L$ . Учитывая высказанное выше соображение (“через  $L$  проходит только  $t$ ”) можно заключить, что существует такое  $m$ , что  $At^m \equiv 0$ . Тогда, согласно предложению (1.3.7),  $A \equiv 0$ , то есть приходим к противоречию с условием. Аналогично разбирается случай, когда  $Q_4 P_3$  образовалось справа от  $R$ .

Остается случай, когда подслово  $Q_4 P_3$  образуется в центре слова, между буквами  $L$  и  $R$ . Учитывая, что “через  $L$  проходит только  $t$ ” и “через  $R$  проходит только  $s$ ”, заключаем, что существуют такие  $m$  и  $l$ , что  $t^m L U R s^l \equiv 0$ .

Теперь к слову  $t^m La^k b^n Q_i P_j M_\varphi H_0 R s^l$  будем применять редукции – определяющие соотношения. Каждая редукция понижает ранг слова. Заметим, что применяемые нами редукции не будут затрагивать  $l$  крайних справа букв  $s$ , так как редукции с участием  $s$  предполагают наличие другой буквы справа от  $s$ . То есть фактически редукции применяются к слову  $t^m La^k b^n Q_i P_j M_\varphi H_0 R$ . Поскольку мы в результате получаем нуль, это доказывает предложение.  $\square$

**Предложение 1.3.9.** Пусть  $\varphi = \varphi(i, j)$ ,  $A = \sum_{f=1}^m \alpha_f t^{p_f} \neq 0$ ,  $B = \sum_{f=1}^l \beta_f s^{q_f} \neq 0$ , и  $ALa^k b^n Q_i P_j M_\varphi H_0 R B \equiv 0$ .

Тогда существует  $N$ , такое, что  $t^N La^k b^n Q_i P_j M_\varphi H_0 R \equiv 0$ .

*Доказательство.* Обозначим  $La^k b^n Q_i P_j M_\varphi H_0 R$  как  $U$ . В выражении  $AUB$  раскроем скобки и будем применять редукции к получившейся сумме мономов. Каждая редукция переводит моном в моном или в нуль. Но если один из мономов редуцируется к нулю, учитывая предложение (1.3.8), получаем, что требуется.

Допустим, таких мономов не найдется. Заметим, что используя определяющие соотношения (редукции) в доказательствах предложений (1.3.1)–(1.3.2), мы можем привести все мономы к виду, не содержащему  $t$ . Таким образом,  $AUB$  редуцируется к виду  $\sum_{f=1}^m \alpha_f U_f s^{p_f} B$ . Слова  $U_f$  не содержат  $t$  и  $s$ , и больше к ним нельзя применить редукции. Так как сумма равна нулю, слагаемые можно разбить на группы (совокупности) подобных, с нулевыми суммами коэффициентов в одной группе. Рассмотрим одну такую группу подобных мономов. Для соответствующих номеров  $f$  все слова  $U_f$  равны. Но тогда равны и соответствующие степени  $t^{p_f}$ . Так как это верно для любой группы, то для общей суммы верно  $A = \sum_{f=1}^m \alpha_f t^{p_f} = 0$ , что противоречит условию.  $\square$

**Предложение 1.3.10.** Пусть слово  $La^k b^n Q_i P_j M_\varphi H_0 R$ , где  $\varphi$  определяется парой  $(i, j)$ , является делителем нуля. Тогда существует  $N$ , такое, что  $t^N La^k b^n Q_i P_j M_\varphi H_0 R \equiv 0$ .

*Доказательство.* Пусть  $La^k b^n Q_i P_j M_\varphi H_0 R$  – делитель нуля. Тогда существуют такие ненулевые элементы алгебры  $A$  и  $B$ , что  $ALa^k b^n Q_i P_j M_\varphi H_0 R B \equiv 0$ . Если оба элемента  $A$  и  $B$  – мономы, используем предложение (1.3.8). Иначе выберем такие  $A$  и  $B$ , что их записи в виде суммы мономов (с коэффициентами), содержат минимальное число

ненулевых мономов:  $A = A_1 + A_2 + \cdots + A_U$ ,  $B = B_1 + B_2 + \cdots + B_V$ . Каждый моном  $A_u$  запишем в виде  $A_u = X_u t^{p_u}$ , где  $p_u$  – неотрицательное целое число. Аналогично, каждый моном  $B_v$  запишем в виде  $B_v = s^{q_v} Y_v$ , где  $q_v$  – неотрицательное целое число. (Во обоих случаях лексикографическое равенство.) То есть мы выделяем степень  $t$  справа от мономов  $A_u$  и степень  $s$  слева от мономов  $B_v$ . Можно считать, что  $X_u$  и  $Y_v$  уже представлены в нормальном виде, не допускающем дальнейших редукций.

Тогда

$$\sum_{1 \leq u \leq U} \sum_{1 \leq v \leq V} X_u t^{p_u} L a^k b^n Q_i P_j M_\varphi H_0 R s^{q_v} Y_v = 0$$

Рассмотрим произвольный моном в этой сумме:

$X t^p L a^k b^n Q_i P_j M_\varphi H_0 R s^q Y$ . Допустим, его можно привести к нулю. Тогда, учитывая предложение (1.3.8), получаем утверждение настоящего предложения. Значит, данный моном можно с помощью редукций привести к нормальному виду (не допускающему дальнейших редукций).  $X$  в начале слова уже в нормальной форме. Заметим, что все редукции, применимы к содержащие  $L$  словам, затрагивают слева от  $L$  только  $t$ . Таким образом,  $X$  в начале слова вообще не затрагивается редукциями, и нормальная форма всего слова начинается с  $X$ . Поскольку это верно для любого монома в сумме, а вся сумма равна нулю, получаем что все  $X_u$  могут быть разделены на несколько групп подобных мономов. Если можно выбрать несколько (но не все) подобных мономов  $X_{u_1} \dots X_{u_s}$  так, что  $\sum_{f=1}^s X_{u_f} t^{p_{u_f}} L a^k b^n Q_i P_j M_\varphi H_0 R s^q \hat{B} = 0$ , то получаем противоречие с минимальностью выбора  $\hat{A}$  и  $\hat{B}$ , так как вместо  $\hat{A}$  можно взять  $\sum_{f=1}^s X_{u_f} t^{p_{u_f}}$ . Значит, несколько таких мономов выбрать нельзя, и группа мономов одна, то есть все мономы  $X_u$  подобны. Тогда их можно вынести за скобки. Внутри скобок остается  $\sum_{f=1}^s t^{p_{u_f}}$ . То есть ситуация сводится к случаю, рассмотренному в предложении (1.3.9).  $\square$

Итак, из предложений (1.3.6) и (1.3.10) следует, что слово  $L a^k b^n Q_i P_j M_\varphi H_0 R$  является делителем нуля тогда и только тогда, когда машина, начав с состояния  $M(i, j, k, n)$  останавливается. Теорема (1.3.1) доказана.

Таким образом, из алгоритмической неразрешимости проблемы остановки универсальной машины следует алгоритмическая неразрешимость вопроса, является ли элемент в алгебре  $\mathbb{A}$  делителем нуля.

## 2. ВСПОМОГАТЕЛЬНЫЕ СВЕДЕНИЯ О МАШИНЕ МИНСКОГО

Будем следовать определению машины Минского, данным М.Сапиром в статье [5]. Пусть имеется две ячейки памяти, в каждой из которых может содержаться одно целое неотрицательное число. Будем называть *программой* конечный набор инструкций, каждая из которых имеет свой уникальный номер.

Каждая *инструкция* принадлежит одному из трех типов:

- (i) Прибавить 1 в ячейку номер  $N$  и далее перейти к инструкции  $j$ .  
 $N \in \{0, 1\}$
- (ii) Если в ячейке номер  $N$  записано число большее нуля, отнять 1 из нее и перейти к инструкции  $j$ , иначе перейти к инструкции  $k$ .  
 $N \in \{0, 1\}$
- (iii) Стоп.

Мы считаем, что программа начинает работать с инструкции 1 и нулем во второй ячейке. Программа заканчивает работать, если в какой-либо момент работы будет выполнена инструкция “СТОП”. Можно считать, что инструкция “СТОП” имеет номер 0.

Мгновенное состояние машины Минского – это тройка  $(n, m, i)$  где  $n, m$  – соответственно, числа хранящиеся в ячейках,  $i$  – номер исполняющейся инструкции.

Таким образом, машина в процессе своей работы каждый тик времени переходит от одного мгновенного состояния к другому. Будем говорить, что машина осуществляет *переход* из состояния  $(n_1, m_1, i)$  в состояние  $(n_2, m_2, j)$  если она, начиная работу с выполнения инструкции  $i$  с записанными числами  $n_1$  в первой ячейке,  $m_1$  во второй ячейке, через некоторое время переходит к выполнению инструкции  $j$ , с записанными числами  $n_2$  в первой ячейке,  $m_2$  во второй ячейке.

Будем говорить, что программа *вычисляет* функцию  $f(n) : \mathbb{N} \rightarrow \mathbb{N}$ , если, для любого натурального  $n$ , начиная с числом  $2^n$  в первой ячейке и нулем во второй, она заканчивает работу с числом  $2^{f(n)}$  в первой ячейке и нулем во второй, то есть осуществляет переход  $(2^n, 0, 1) \rightarrow (2^{f(n)}, 0, 0)$ .

Соответственно, будем называть функцию  $f(n) : \mathbb{N} \rightarrow \mathbb{N}$  *вычислимой по Минскому*, если существует машина Минского, вычисляющая данную функцию.

Заметим, что одним хранящимся в ячейке числом можно кодировать несколько чисел. Например, мы можем хранить в первой ячейке пару чисел  $(n, m)$  как число  $2^k \times 3^m$ . С учетом этого, появляется возможность хранить в одной ячейке целый набор чисел.

При этом, степенью каждого простого числа можно пользоваться как отдельным регистром памяти. Будем называть регистры аналогично простым числам, степени которых являются их значения. Например, регистры **2**, **3**, **5**. Также, приведенная конструкция позволяет определить вычислимые функции многих переменных.

Например, машина вычисляет сумму, если она для любых натуральных чисел  $n, m$  осуществляет переход  $(2^n \times 3^m, 0, 1) \rightarrow (2^{n+m}, 0, 0)$ .

Нашей основной целью будет создать машину Минского, вычисляющую  $[n^\alpha]$  для рекурсивного числа  $\alpha$ , то есть придумать программу, осуществляющую переход  $(2^n, 0, 1) \rightarrow (2^{[n^\alpha]}, 0, 0)$ , где  $[x]$  – целая часть  $x$ .

Для этого сначала опишем несколько более простых переходов, чтобы затем из них сформировать нужный нам.

Сразу отметим, что мы можем прибавлять к ячейке любое наперед заданное натуральное число, не только единицу. Это реализуется посредством следующей подпрограммы:

### прибавление $k$

**i<sub>0</sub>**. СТОП.

**i<sub>1</sub>**. Прибавить 1 к ячейке 1, перейти к  $i_2$ .

**i<sub>2</sub>**. Прибавить 1 к ячейке 1, перейти к  $i_3$ .

...

$i_k$ . Прибавить 1 к ячейке 1, перейти к  $i_0$ .

Заметим, что мы можем вставить данную подпрограмму (кроме нулевой строки) в текст другой программы. Затем, когда нам нужно прибавить  $k$ , вызывать данную подпрограмму. Под номером  $i_0$  мы подразумеваем первую инструкцию, которая должна быть исполнена после выполнения подпрограммы. То есть, команда СТОП для подпрограммы означает выход из нее. Отметим, что текст программы очевидным образом можно изменить, чтобы прибавлять ко второй ячейке.

В дальнейшем, мы будем использовать *макрокоманды* – представляющие собой подпрограммы, осуществляющие некоторое действие, для которого программа уже написана. То есть, теперь мы можем использовать команду “прибавить  $k$  к первой (второй) ячейке”.

Аналогично, можно построить еще несколько примеров подпрограмм.

Покажем, что машина может делить и умножать число в ячейке на два и три, а также проверять, делится ли число в ячейке на два и три.

### **умножение на два (прибавление единицы в регистр)**

**i<sub>0</sub>**. СТОП.

**i<sub>1</sub>**. Отнять 1 из ячейки-1, перейти к  $i_2$ , если в первой ячейке 0, перейти к  $i_3$ .

**i<sub>2</sub>**. Прибавить 2 к ячейке-2, перейти к  $i_1$ .

**i<sub>3</sub>**. Отнять 1 из ячейки-2, перейти к  $i_4$ , если во второй ячейке 0, перейти к  $i_0$ .

**i<sub>4</sub>**. Прибавить 1 к ячейке-1, перейти к  $i_3$ .

Приведенная программа осуществляет переход  $(k, 0, i_1) \rightarrow (0, 2k, i_3) \rightarrow (2k, 0, i_0)$ . Аналогично можно построить программу, умножающую число в ячейке на любое наперед заданное число.

Теперь покажем, как реализовать макрокоманду:

“Если число в ячейке 1 делится на 2, разделить и перейти к  $i_{0_1}$ , если нет – перейти к  $i_{0_2}$ .”

### **деление на два (вычитание единицы из регистра).**

**i<sub>0\_1</sub>**. СТОП 1.

**i<sub>0\_2</sub>**. СТОП 2.

**i<sub>1</sub>**. Отнять 1 из ячейки-1, перейти к  $i_2$ , если в первой ячейке 0, перейти к  $i_4$ .

**i<sub>2</sub>**. Отнять 1 из ячейки-1, перейти к  $i_3$ , если в первой ячейке 0, перейти к  $i_6$ .

**i<sub>3</sub>**. Прибавить 1 к ячейке-2, перейти к  $i_1$ .

**i<sub>4</sub>**. Отнять 1 из ячейки-2, перейти к  $i_5$ , если во второй ячейке 0, перейти к  $i_{0_1}$ .

**i<sub>5</sub>**. Прибавить 1 к ячейке-1, перейти к  $i_4$ .

**i<sub>6</sub>**. Прибавить 1 к ячейке-1, перейти к  $i_7$ .

**i<sub>7</sub>**. Отнять 1 из ячейки-2, перейти к  $i_8$ , если во второй ячейке 0, перейти к  $i_{0_2}$ .

**i<sub>8</sub>**. Прибавить 2 к ячейке-1, перейти к  $i_7$ .

В случае, если число  $k$  в первой ячейке делится на два, данная программа реализует переход:  $(k, 0, i_1) \rightarrow (0, \frac{k}{2}, i_4) \rightarrow (\frac{k}{2}, 0, i_{0_1})$ .

Если же число  $k$  в первой ячейке не делится на два, реализуется переход:  $(k, 0, i_1) \rightarrow (0, \frac{k-1}{2}, i_2) \rightarrow (1, \frac{k-1}{2}, 0, i_7) \rightarrow (k, 0, i_{0_2})$ .

Отметим, что очевидные изменения позволяют осуществить аналогичное деление на любое наперед заданное число.

Приведем пример программы, осуществляющей переход  $(2^n, 0, 1) \rightarrow (2^n3^n, 0, 0)$ .

### Копирование регистра

**i<sub>0</sub>**. СТОП.

**i<sub>1</sub>**. Разделить число в первой ячейке на два и перейти к  $i_2$ . Если не делится, перейти к  $i_3$ .

**i<sub>2</sub>**. Умножить число во первой ячейке на 15, перейти к  $i_1$ .

**i<sub>3</sub>**. Разделить число в первой ячейке на 5 и перейти к  $i_4$ . Если не делится, перейти к  $i_0$ .

**i<sub>4</sub>**. Умножить число во первой ячейке на 2, перейти к  $i_3$ .

Приведенная программа осуществляет переход  $(2^k m, 0, i_1) \rightarrow (3^k 5^k m, 0, i_3) \rightarrow (3^k 2^k m, 0, i_0)$ .

Здесь  $m$  не делится на два, три, пять.

### Сложение регистров

**i<sub>0</sub>**. СТОП.

**i<sub>1</sub>**. Разделить число в первой ячейке на три и перейти к  $i_2$ . Если не делится, перейти к  $i_3$ .

**i<sub>2</sub>**. Умножить число во первой ячейке на 10, перейти к  $i_1$ .

**i<sub>3</sub>**. Разделить число в первой ячейке на 5 и перейти к  $i_4$ . Если не делится, перейти к  $i_0$ .

**i<sub>4</sub>**. Умножить число во первой ячейке на 3, перейти к  $i_3$ .

Приведенная программа осуществляет переход  $(2^k 3^n m, 0, i_1) \rightarrow (2^{k+n} 5^n m, 0, i_3) \rightarrow (2^{k+n} 3^n m, 0, i_0)$ .

Здесь  $m$  не делится на два, три, пять.

В дальнейшем, под словами “прибавить к содержимому регистра **2** содержимое регистра **3**” будем предполагать только что описанную подпрограмму. Ясно, что ее можно очевидным образом изменить, для вычисления суммы любой другой пары регистров.

## Умножение регистров

**i<sub>0</sub>**. СТОП.

**i<sub>1</sub>**. Скопировать регистр **2** в регистр **5**, перейти к  $i_2$ .

**i<sub>2</sub>**. Вычесть единицу из регистра **2**, перейти к  $i_2$ . Если в регистре **2** записан нуль, перейти к  $i_3$ .

**i<sub>3</sub>**. Вычесть единицу из регистра **5**, перейти к  $i_4$ . Если в регистре **5** записан нуль, перейти к  $i_0$ .

**i<sub>4</sub>**. Прибавить к содержимому регистра **2** содержимое регистра **3**, перейти к  $i_3$ .

Приведенная программа осуществляет переход  $(2^k 3^n m, 0, i_1) \rightarrow (2^k 3^n 5^k m, 0, i_2) \rightarrow (3^n 5^k m, 0, i_3) \rightarrow (2^n 3^n 5^{k-1} m, 0, i_3) \rightarrow (2^{2n} 3^n 5^{k-2} m, 0, i_3) \rightarrow \dots \rightarrow (2^{kn} 3^n m, 0, i_0)$ .

Здесь  $m$  не делится на два, три, пять.

В дальнейшем, под словами “умножить содержимое регистра **2** на содержимое регистра **3**” будем предполагать только что описанную подпрограмму. Ясно, что ее можно очевидным образом изменить, для вычисления произведения любой другой пары регистров.

Теперь опишем подпрограмму для сравнения регистров. Если число в регистре **2** меньше либо равно числу в регистре **3**, подпрограмма останавливается в на команде СТОП 1, иначе на команде СТОП 2.

## Сравнение регистров

**i<sub>01</sub>**. СТОП 1.

**i<sub>02</sub>**. СТОП 2.

**i<sub>1</sub>**. Вычесть единицу из регистра **2**, перейти к  $i_2$ . Если в регистре **2** записан нуль, перейти к  $i_{01}$ .

**i<sub>2</sub>**. Вычесть единицу из регистра **3**, перейти к  $i_1$ . Если в регистре **3** записан нуль, перейти к  $i_{02}$ .

Приведенная программа осуществляет переход  $(2^k 3^n m, 0, i_1) \rightarrow (2^{k-1} 3^{n-1} m, 0, i_1) \rightarrow (2^{k-2} 3^{n-2} m, 0, i_1) \rightarrow \dots$ . Здесь  $m$  не делится на два и три.

### Очистка регистра

**i<sub>0</sub>**. СТОП.

**i<sub>1</sub>**. Вычесть единицу из регистра **2**, перейти к  $i_1$ . Если в регистре **2** записан нуль, перейти к  $i_0$ .

Приведенная программа осуществляет переход  $(2^k m, 0, i_1) \rightarrow (m, 0, i_1)$ .

Здесь  $m$  не делится на два.

Теперь приведем программу для вычисления степени  $(2^k 3^n, 0, 1) \rightarrow (2^{k^{2^n}} 3^n, 0, 1)$ . То есть данная программа возводит регистр **2** в степень 2 столько раз, каково содержимое регистра **3**. Ясно, что можно перенумеровать регистры и использовать программу и для других пар регистров.

### Вычисление $2^n$ -степени

**i<sub>0</sub>**. СТОП.

**i<sub>1</sub>**. Скопировать регистр **3** в регистр **5**, перейти к  $i_2$ .

**i<sub>2</sub>**. Вычесть единицу из регистра **5**, перейти к  $i_3$ . Если в регистре **5** записан нуль, перейти к  $i_0$ .

**i<sub>3</sub>**. Умножить содержимое регистра **2** на содержимое регистра **2**, перейти к  $i_2$ .

Приведенная программа осуществляет переход  $(2^k 3^n m, 0, i_1) \rightarrow (2^k 3^n 5^n m, 0, i_2) \rightarrow (2^{k^2} 3^n 5^{n-1} m, 0, i_2) \rightarrow \dots \rightarrow (2^{k^{2^n}} 3^n m, 0, i_0)$ .

Здесь  $m$  не делится на два, три и пять.

Следующая программа вычисляет корень  $2^n$ -степени. Мы последовательно увеличиваем число-кандидат на значение корня, каждый раз возводя его в  $2^n$ -степень и сравнивая с  $k$ . Если в некий момент получаем число большее  $k$ , отнимаем от числа кандидата единицу и получаем ответ.

### Вычисление корня $2^n$ -степени

**i<sub>0</sub>**. СТОП.

**i<sub>1</sub>**. Очистить регистр **7**, перейти к  $i_2$ .

- i<sub>2</sub>**. Очистить регистр **5**, перейти к  $i_3$ .
- i<sub>3</sub>**. Скопировать регистр **7** в регистр **5**, перейти к  $i_4$ .
- i<sub>4</sub>**. Увеличить регистр **5** на единицу, перейти к  $i_5$ .
- i<sub>5</sub>**. Возвести содержимое регистра **5** в степень  $2^n$ , где  $n$  – содержимое регистра **3**, перейти к  $i_7$ .
- i<sub>6</sub>**. Сравнить регистр **5** с регистром **2**. Если содержимое регистра **2** больше, перейти к  $i_7$ , иначе, перейти к  $i_8$ .
- i<sub>7</sub>**. Увеличить регистр **7** на единицу, перейти к  $i_2$ .
- i<sub>8</sub>**. Очистить регистр **2**, перейти к  $i_9$ .
- i<sub>9</sub>**. Скопировать регистр **7** в регистр **2**, перейти к  $i_{10}$ .
- i<sub>10</sub>**. Очистить регистр **5**, перейти к  $i_{11}$ .
- i<sub>11</sub>**. Очистить регистр **7**, перейти к  $i_0$ .

Приведенная программа осуществляет переход  $(2^k 3^n m, 0, i_1) \rightarrow (2^k 3^{n+1} m, 0, i_5) \rightarrow (2^k 3^n 5^1 m, 0, i_5) \rightarrow (2^k 3^n 5^2 7^1 m, 0, i_5) \rightarrow \dots \rightarrow (2^k 3^n 5^{[k^{\frac{1}{2^n}}]+1}, 7^{[k^{\frac{1}{2^n}}]} m, 0, i_6) \rightarrow (2^{[k^{\frac{1}{2^n}}]} 3^n m, 0, i_0)$ .

Здесь  $m$  не делится на два, три, пять и семь.

**Определение 2.0.2.** Пусть  $\alpha$  – вещественное число, имеющее представление в виде суммы степеней двойки:  $\alpha = \sum_{i=1}^{\infty} \alpha_i 2^{-i}$ , где  $\alpha_i \in \{0, 1\}$ .  $\alpha$  называется рекурсивным, если существует машина Минского, осуществляющая переход  $(2^i, 0, 1) \rightarrow (2^i 3^{\alpha_i}, 0, 0)$  универсально по  $i$ .

Пусть  $\alpha$  – рекурсивное число. Согласно определению, мы обладаем подпрограммой, вычисляющей его заданную цифру в двоичной записи.

Ясно, что для любого  $n$  существует  $h$ , такое, что  $[n^\alpha] = [n^{\sum_{i=1}^{\infty} \alpha_i 2^{-i}}] = [n^{\sum_{i=1}^h \alpha_i 2^{-i}}]$ , то есть бесконечную сумму для данного числа  $n$  можно заменить конечным отрезком. Конечную сумму можно привести к общему знаменателю:  $\sum_{i=1}^h \alpha_i 2^{-i} = \frac{r}{2^h}$

Тогда  $[n^\alpha] = [n^{\frac{r}{2^h}}]$ . Таким образом, задача возведения в рекурсивную степень сводится к задаче возведения в подходящую рациональную степень.

Теперь приведем программу, вычисляющую число  $r$  и  $h$  из формулы  $[n^\alpha] = [n^{\frac{r}{2^h}}]$ .

## Вычисление числителя приближающей дроби

**i<sub>0</sub>**. СТОП.

**i<sub>1</sub>**. Очистить регистры **3**, **7**, **11**, перейти к  $i_2$ .

**i<sub>2</sub>**. Очистить регистр **5**, перейти к  $i_3$ .

**i<sub>3</sub>**. Скопировать регистр **2** в регистр **5**, перейти к  $i_4$ .

**i<sub>4</sub>**. Увеличить регистр **3** на единицу, перейти к  $i_5$ .

**i<sub>5</sub>**. Извлечь из содержимого регистра **5** корень степени  $2^n$ , где  $n$  – содержимое регистра **3**, перейти к  $i_6$ .

**i<sub>6</sub>**. Прибавить к содержимому регистра **7** содержимое регистра **7** (удвоить), перейти к  $i_7$ .

**i<sub>7</sub>**. Вычислить  $n$ -ую цифру в двоичной записи  $\alpha$ , где  $n$  – содержимое регистра **3**, записать ее в регистр **11**, перейти к  $i_8$ .

**i<sub>8</sub>**. Вычесть единицу из регистра **11**, перейти к  $i_9$ . Если в регистре **11** записан нуль, перейти к  $i_{10}$ .

**i<sub>9</sub>**. Увеличить регистр **7** на единицу, перейти к  $i_{10}$ .

**i<sub>10</sub>**. Вычесть единицу из регистра **5**, перейти к  $i_{11}$ . Если в регистре **5** записан нуль, перейти к  $i_{11}$ .

**i<sub>11</sub>**. Вычесть единицу из регистра **5**, перейти к  $i_2$ . Если в регистре **5** записан нуль, перейти к  $i_{12}$ .

**i<sub>12</sub>**. Очистить регистры **5**, **11**, перейти к  $i_0$ .

Приведенная программа осуществляет переход  $(2^k m, 0, i_1) \rightarrow (2^k 3^1 5^k m, 0, i_5) \rightarrow (2^k 3^2 5^k 7^{\alpha_1} m, 0, i_5) \rightarrow \dots \rightarrow (2^k 3^h 5^1 7^r m, 0, i_{10}) \rightarrow (2^k 3^h 7^r m, 0, i_0)$ .

Здесь  $m$  не делится на два, три, пять, семь и одиннадцать.

Таким образом, мы можем вычислить числитель и знаменатель дроби, приближающей число  $\alpha$  для данного основания  $n$ .

Тогда можно написать программу для вычисления  $[n^\alpha]$ . Итак, в начале в регистре **2** записано число  $n$ .

## Вычисление $[n^\alpha]$

**i<sub>0</sub>**. СТОП.

**i<sub>1</sub>**. Очистить регистры **3**, **5**, **5**, перейти к  $i_2$ .

- i<sub>2</sub>.** Вычислить  $r$  и  $h$  из формулы  $[n^\alpha] = [n^{\frac{r}{2^h}}]$ , поместив  $h$  в регистр **3**,  $r$  в регистр **5**, перейти к  $i_3$ .
- i<sub>3</sub>.** Прибавить единицу в регистр **7**, перейти к  $i_4$ .
- i<sub>4</sub>.** Вычесть единицу из регистра **5**, перейти к  $i_5$ . Если в регистре **5** записан нуль, перейти к  $i_6$ .
- i<sub>5</sub>.** Умножить содержимое регистра **7** на содержимое регистра **2**, перейти к  $i_4$ .
- i<sub>6</sub>.** Извлечь из содержимого регистра **7** корень степени  $2^h$ , где  $h$  – содержимое регистра **3**, перейти к  $i_7$ .
- i<sub>7</sub>.** Скопировать содержимое регистра **7** в регистр **2**, перейти к  $i_8$ .
- i<sub>8</sub>.** Очистить регистры **7**, **3**, перейти к  $i_0$ .

Приведенная программа осуществляет переход

$$(2^n, 0, i_1) \rightarrow (2^n 3^h 5^r 7^1, 0, i_4) \rightarrow (2^k 3^h 5^{r-1} 7^n m, 0, i_4) \rightarrow \dots$$

$$\dots \rightarrow (2^k 3^h 5^0 7^{n^r}, 0, i_4) \rightarrow (2^k 3^h 7^{[n^{\frac{r}{2^h}}]}, 0, i_7) \rightarrow (2^{[n^{\frac{r}{2^h}}]}, 0, i_0).$$

Таким образом, машина Минского позволяет производить возведение в рекурсивную степень, с округлением в сторону меньшего целого.

### 3. РЕАЛИЗАЦИЯ МАШИНЫ МИНСКОГО В КОНЕЧНО-ОПРЕДЕЛЕННОЙ ПОЛУГРУППЕ

Сначала необходимо ввести несколько определений.

**Определение 3.0.3.** Пусть  $S$  – полугруппа порожденная конечным множеством букв  $\{s_1, \dots, s_m\}$ .

Пусть  $U^n$  – множество всевозможных слов  $r_{i_1} \dots r_{i_n}$ , где  $i_j = 1, \dots, m$ .  $n = 0, 1, 2, \dots$ . Тогда  $U^n \in S$  и  $U^n$  состоит из слов длины  $n$ . Пусть  $g_U(n)$  это число неэквивалентных слов в  $U^1 \bigcup U^2 \bigcup \dots \bigcup U^n$ .

$g_U(n)$  называется *функцией роста* полугруппы  $S$

**Определение 3.0.4.** Размерность Гельфанд–Кириллова полугруппы  $S$  определяется как

$$\text{GKdim}(S) = \limsup_{n \rightarrow \infty} (\log_n g_U(n)) = \limsup_{n \rightarrow \infty} \frac{\log g_U(n)}{\log n}.$$

Хорошо известно следующее предложение.

**Предложение 3.0.11.** Размерность Гельфанд–Кириллова не зависит от выбора переменных.

В настоящей главе будет доказана следующая теорема.

**Теорема 3.0.2.** Существует конечно-определенная полугруппа с нецелой размерностью Гельфанд–Кириллова.

#### 3.1 План построения полугруппы с полуцелой размерностью Гельфанд–Кириллова.

В основе построения лежит следующая модель: каждому элементу полугруппы отвечает четверка неотрицательных целых чисел и состояние (одно из двух). Первая пара чисел (они моделируются степенями букв  $a$  и  $b$ ) и состояние, является интерпретацией машины Минского. С помощью машины Минского мы обрабатываем другую пару чисел (они моделируются степенями букв  $s$  и  $t$ ), проверяя, что количество  $t$  выражается

квадратичной формулой. При этом мы используем факт, что число букв в ненулевом слове не меняется при переходе к эквивалентному слову.

Пару чисел  $(n, k)$ , представляющую число вхождений  $a$  и  $b$  удобно представлять себе в виде точки на целочисленной решетке с координатами  $(n, k)$ . Таким образом, переход к эквивалентному слову соответствует переходу в соседнюю точку решетки. Кроме того, мы задаем определяющие соотношения таким образом, что существует единственный способ перемещения по четверти плоскости – вдоль заданного пути обхода:

$$(0, 0) - (1, 0) - (0, 1) - (0, 2) - (1, 1) - (2, 0) - (3, 0) - (2, 1) - \dots$$

Либо по зеркально симметричному относительно диагонали пути, причем для каждого слова возможен лишь один путь. Таким образом, делаются ходы вдоль границы (*внешние ходы*)  $(n, 0) - (n + 1, 0)$ ,  $(0, n) - (0, n + 1)$ , а также *внутренние ходы*  $(n, k) - (n + 1, k - 1)$ .

При перемещении из точки  $(0, 0)$  вдоль заданного пути в точку  $(n, k)$  количество внутренних ходов квадратично относительно количества внешних. За счет этого мы добиваемся квадратичного количества вхождений одной из букв относительно другой.

В дальнейшем, латинские буквы  $n, k, m, l, p, q, i, j$  обозначают целые неотрицательные числа, причем будет указываться, в каких пределах они могут изменяться. Греческие буквы  $\alpha, \gamma, \beta$  обычно равны либо 0 либо 1. Все они будут использоваться для обозначения степеней букв в словах.

### 3.2 Определяющие соотношения.

Пусть задан алфавит  $\Omega$ :

$$\{L, R, a, b, t, s, Q_1, Q_2, u, g, f, h, v\}.$$

Рассмотрим полугруппу с нулем  $S$ , порожденную словами в этом алфавите. Нашей целью будет задание конечного числа определяющих соотношений, создающих необходимую нам структуру на полугруппе  $S$ . В частности, нас будет особенно интересовать наличие канонической формы на полугруппе  $S$ : любое слово, не отвечающее канонической форме, равно нулю.

Рассмотрим следующее множество соотношений:

$$xL = 0; \quad \text{где } x - \text{любая буква кроме } L \quad (3.1)$$

$$Rx = 0; \quad \text{где } x - \text{любая буква кроме } R \quad (3.2)$$

$$sR = 0; \quad (3.3)$$

$$Lx = 0; \quad \text{где } x - \text{любая буква кроме } \{L, a, Q_i, s\} \quad (3.4)$$

$$ax = 0; \quad x - \text{любая буква кроме } \{a, s, Q_i, u\} \quad (3.5)$$

$$xa = 0; \quad \text{где } x - \text{любая буква кроме } \{L, a, s, u\} \quad (3.6)$$

$$xQ_i = 0; \quad \text{где } x - \text{любая буква кроме } \{L, a, s, u\} \quad (3.7)$$

$$Q_i x = 0; \quad \text{где } x - \text{любая буква кроме } \{b, t, s, g, h, u\} \quad (3.8)$$

$$gx = 0; \quad \text{где } x - \text{любая буква, кроме } \{f, b, h, v, R, u\} \quad (3.9)$$

$$fx = 0; \quad \text{где } x - \text{любая буква, кроме } \{f, b, h, v, R, u\} \quad (3.10)$$

$$xf = 0; \quad \text{где } x - \text{любая буква, кроме } \{f, g, b, v, h, u\} \quad (3.11)$$

$$hx = 0; \quad \text{где } x - \text{любая буква, кроме } \{f, g, t, v, R, u\} \quad (3.12)$$

$$vx = 0; \quad \text{где } x - \text{любая буква, кроме } \{f, g, t, v, R, u\} \quad (3.13)$$

$$xv = 0; \quad \text{где } x - \text{любая буква, кроме } \{f, g, t, v, h, u\} \quad (3.14)$$

$$us = uL = 0; \quad (3.15)$$

$$ux = xu; \quad \text{где } x - \text{любая буква кроме } \{L, R, s\} \quad (3.16)$$

$$sx = xs; \quad \text{где } x - \text{любая буква кроме } \{L, R, g, h, u\} \quad (3.17)$$

$$tx = xt; \quad \text{где } x \in \{b, s, h, v, u\} \quad (3.18)$$

$$gx = xg; \quad \text{где } x \in \{b, h, v, u\} \quad (3.19)$$

$$hx = xh; \quad \text{где } x \in \{t, g, f, u\} \quad (3.20)$$

$$fx = xf; \quad \text{где } x \in \{b, h, v, u\} \quad (3.21)$$

$$vx = xv; \quad \text{где } x \in \{t, g, f, u\} \quad (3.22)$$

$$R^2 = fR; \quad (3.23)$$

$$R^2 = vR; \quad (3.24)$$

$$R^2 = uR; \quad (3.25)$$

$$LQ_1t = LQ_2b; \quad (3.26)$$

$$Q_2bt = aQ_2s; \quad (3.27)$$

$$Q_2th = aQ_1h; \quad (3.28)$$

$$aQ_1t = Q_1bs; \quad (3.29)$$

$$aQ_i bg = 0. \quad (3.30)$$

### 3.3 Приведение к каноническому виду.

Для приведения к каноническому виду нам потребуется несколько лемм.

**Предложение 3.3.1.** *Любое ненулевое слово имеет вид  $L^nXR^k$ , где  $X$  не содержит  $L$  и  $R$ ,  $n, k \geq 0$ .*

Если в слове нет букв  $L$  и  $R$ , то оно уже имеет требуемый вид при  $n = k = 0$ . Пусть в слове имеется буква  $L$ . Согласно соотношению (3.1), левее  $L$  должны быть тоже  $L$ , таким образом, слово имеет вид  $L^nY$ , где слово  $Y$  не содержит  $L$ . Теперь, если в слове есть  $R$ , учитывая соотношение (3.2), получаем что слово представляется в требуемом виде.

**Предложение 3.3.2.** *Если  $W \neq 0$ , то  $W \equiv Xf^kv^n u^m$ ,*

*где  $X$  не содержит  $f$ ,  $v$ ,  $u$ , кроме того,  $k, n, m \geq 0$ . Причем, если в слове  $W$  содержится хотя бы одна буква  $R$ , то  $W$  приводится к виду, не содержащему  $f$ ,  $u$ ,  $v$ .*

Согласно предложению (3.3.1), можно считать, что  $W = UR^n$ , где  $U$  не содержит  $R$ , и  $n \geq 0$ .

Рассмотрим слово  $U$ . Если в  $U$  нет букв  $f$ ,  $v$ ,  $u$ , то  $W$  уже имеет требуемый вид.

Пусть, например, в  $U$  имеются одна или несколько букв  $f$ . Выберем крайнее справа вхождение. Слово  $U$  имеет вид  $X_1fX_2$ , где  $X_2$  не содержит  $f$ . Так как  $U \neq 0$ , то согласно соотношению (3.10), первой буквой в слове  $X_2$  могут быть только буквы  $b, h, v, u$ . (Букв  $R$  и  $f$  слово  $X_2$  не содержит.) Используя, что  $f$  коммутирует с  $b, h, v, u$  – соотношение (3.21), получаем, что  $U \equiv X_1X_2f$ . Теперь выберем крайнее справа вхождение  $f$  в слово  $X_1X_2$  и проведем аналогичные операции. Проведя указанные действия со всеми вхождениями  $f$  в слово  $U$ , мы приведем  $U$  к виду  $X_3f^k$ , где  $k \geq 0$ .

Пусть, теперь, в  $U$  имеются одна или несколько букв  $v$ . Выберем крайнее справа вхождение. Слово  $U$  имеет вид  $Y_1vY_2$ , где  $Y_2$  не содержит  $v$ . Так как  $U \neq 0$ , то согласно соотношению (3.13), первой буквой в слове  $Y_2$  могут быть только буквы  $b, h, f, u$ . (Букв  $R$  и  $v$  слово  $Y_2$  не содержит.) Используя, что  $v$  коммутирует с  $b, h, f, u$  – соотношение (3.22), получаем, что  $U \equiv Y_1Y_2v$ . Теперь выберем крайнее справа вхождение  $v$  в слово  $Y_1Y_2$  и проведем аналогичные операции. Проведя указанные действия со всеми вхождениями  $v$  в слово  $U$ , мы приведем  $U$  к виду  $Y_3v^n$ , где  $n \geq 0$ .

Пусть, теперь, в  $U$  имеются одна или несколько букв  $u$ . Выберем крайнее справа вхождение. Слово  $U$  имеет вид  $Z_1uZ_2$ , где  $Z_2$  не содержит  $u$ . Так как  $U \neq 0$ , то согласно соотношению (3.15), первой буквой в слове  $Z_2$  может быть любая буква кроме  $L, R, u, s$ . (Букв  $R$  и  $u$  слово  $Z_2$  не содержит.) Используя, что  $u$  коммутирует с всеми буквами, кроме  $L, R, s$  – соотношение (3.16), получаем, что  $U \equiv Z_1Z_2u$ . Теперь выберем крайнее справа вхождение  $u$  в слово  $Z_1Z_2$  и проведем аналогичные операции. Проведя указанные действия со всеми вхождениями  $u$  в слово  $U$ , мы приведем  $U$  к виду  $Z_3u^m$ , где  $m \geq 0$ .

Заметим, что буквы  $u, v, f$  коммутируют между собой.

Возвращаясь к рассмотрению всего слова  $W$ , получаем, что

$$W \equiv Xf^k v^n u^m R^l, \text{ где } X \text{ не содержит } f, v, u \text{ и } k, n, m > 0, l \geq 0.$$

Теперь, если  $l = 0$ , то есть если  $W$  не содержит  $R$ , то мы уже получили требуемый вид. Если же в слове содержится хотя бы одна буква  $R$  ( $l \geq 1$ ), то мы используем  $R^2 = uR = vR = fR$  – соотношения (3.23), (3.24), (3.25) и получаем

$W \equiv Xf^k v^n u^m R^l \equiv X R^{k+n+l+m}$ . В этом случае  $W$  приводится к виду, не содержащему  $f, v, u$ .

Таким образом, получаем утверждение леммы.

**Предложение 3.3.3.** *Любое ненулевое слово  $W$ , не содержащее  $R$  имеет вид  $Xg^\alpha h^\beta f^k v^n u^m$ ,*

*где  $X$  не содержит  $h, g, f, v, u$ ; кроме того,  $k, n, m \geq 0$ , а также  $\alpha, \beta \in \{0, 1\}$*

Согласно предложению (3.3.2), слово  $W$  можно представить в виде  $Xf^k v^n u^m$ , где  $X$  не содержит  $f, v, u$ . Рассмотрим слово  $X$ . Если в нем нет букв  $g$  и  $h$ , то оно уже имеет требуемый вид при  $\alpha = \beta = 0$ . Пусть, например, в слове имеются одна или несколько букв  $g$ . Возьмем крайнее левое вхождение. Тогда слово  $X$  имеет вид  $X_1gX_2$ , где  $X_1$  не содержит  $g$ . Согласно соотношению (3.9), первой буквой в слове  $X_2$  могут быть только буквы  $b, h, u, f, v, R$ . Заметим, что  $g$  коммутирует с  $b, h$  – Соотношение (3.19), а  $f, v, u, R$  в слове  $X_2$  не встречаются. Таким образом, можно продвинуть  $g$  на одну букву вправо. Теперь опять рассмотрим букву справа от  $g$ . Аналогично заключаем, что это может быть только  $b$  или  $h$ . Продолжая в том же духе, получаем, что  $X \equiv X_3g$ , где  $X_3$  не содержит  $g$ .

Пусть теперь в слове имеются одна или несколько букв  $h$ . Возьмем крайнее левое вхождение. Тогда слово  $X$  имеет вид  $Y_1hY_2$ , где  $Y_1$  не со-

держит  $h$ . Согласно соотношению (3.12), первой буквой в слове  $Y_2$  могут быть только буквы  $t, g, u, f, v, R$ . Заметим, что  $h$  коммутирует с  $t, g$ , – соотношение (3.20), а  $f, v, u, R$  в слове  $Y_2$  не встречаются. Таким образом, можно продвинуть  $g$  на одну букву вправо. Теперь опять рассмотрим букву справа от  $g$ . Аналогично заключаем, что это может быть только  $t$  или  $g$ . Продолжая в том же духе, получаем, что  $X \equiv Y_3h$ , где  $Y_3$  не содержит  $h$ .

В итоге получаем требуемый вид.

**Предложение 3.3.4.** *Любое ненулевое слово  $W$ , не содержащее  $L, R, Q_1, Q_2$  может быть представлено в одной из следующих форм:*

- (i)  $s^n a^m u^j$ ;
  - (ii)  $s^n b^k t^m g^\alpha h^\beta f^l v^i u^j$ ,
- где  $n, k, m, l, i, j \geq 0$ , кроме того,  $\alpha, \beta \in \{0, 1\}$ .

Согласно предложению (3.3.3),  $W$  можно привести к виду  $X g^\alpha h^\beta f^l v^i u^j$ , где  $X$  не содержит  $h, g, f, v, u$ , а также  $\alpha, \beta \in \{0, 1\}$ .

Таким образом,  $X$  содержит лишь буквы  $a, b, t, s$ . Заметим, что  $s$  коммутирует с остальными буквами этой четверки – соотношение (3.17), произведение  $a$  и  $b$  (или  $t$ ) равно нулю – соотношения (3.5), (3.6) и  $b$  и  $t$  коммутируют – соотношение (3.18). Из этого следует, что  $X \equiv s^n a^m$  или  $X \equiv s^n b^k t^m$ . Если имеет место первый вариант, то букв  $g, h, f, v$  в слове быть уже не может, иначе оно приводится к нулю с помощью соотношения (3.5). Таким образом, получаем утверждение леммы.

**Предложение 3.3.5.** *Пусть ненулевое слово  $W$  не содержит  $Q_i, i \in \{1, 2\}$ . Тогда:*

- (i) *Если  $W$  содержит  $L$ , то оно представляется в одном из следующих видов:*
  1.  $L^l s^n a^k u^m$ , где  $n, k, m \geq 0, l \geq 1$ , если  $m > 0$ , то  $n > 0$ ;
  2.  $L^l s^n g^\alpha h^\beta f^p v^i u^j$ ,

где  $\alpha, \beta \in \{0, 1\}$ , кроме того  $p, i, j \geq 0, n, l \geq 1$ , если  $p > 0$ , то  $\alpha = 1$ , если  $i > 0$ , то  $\beta = 1$ .
- (ii) *Если  $W$  содержит  $R$ , то оно представляется в одном из следующих видов:*
  1.  $s^n b^m t^l g^\alpha h^\beta R$ , где  $n, m, l \geq 0$ , кроме того  $\alpha, \beta \in \{0, 1\}$ .

2.  $b^m h R^k$ , где  $m \geq 0, k \geq 2$ ;
3.  $t^l g R^k$ , где  $l \geq 0, k \geq 2$ ;
4.  $s^n b^m t^l g h R^k$ , где  $n, m, l \geq 0, k \geq 2$ .

(iii) Если  $W$  содержит  $L, R$ , то оно представляется в одном из следующих видов:

1.  $L^l s^n g h R^k$ , где  $l, n > 0, k > 1$ ;
2.  $L^l s^n g^\alpha h^\beta R$ , где  $l, n > 0$ , кроме того  $\alpha, \beta \in \{0, 1\}$ .

(i) По предложению (3.3.1),  $W = L^l X$ ,  $X$  не содержит  $L$  и  $R$ . Применяя к  $X$  предложение (3.3.4), получаем, что  $W \equiv L^l s^n a^k u^m$  или  $W \equiv L^l s^n b^m t^k g^\alpha h^\beta f^p v^i u^j R^k$ , где  $n, m, k, p, i, j \geq 0, l \geq 1$ , а также  $\alpha, \beta = 0$  или 1.

В первом случае, если  $m > 0$  то есть если  $u$  присутствует в слове, то должна быть хотя бы одна  $s$ , иначе слово приводится к нулю с помощью  $ua = au, Lu = 0$  – соотношения (3.4), (3.16).

Во втором случае  $m = k = 0$ , то есть буквы  $b, t$  в слове отсутствуют, иначе оно приводится к нулю с помощью  $st = ts, sb = bs, Lb = Lt = 0$  – соотношения (3.4), (3.17). Кроме того, если в слове присутствует хотя бы одна из букв  $g, h, f, v, u$ , то также должна присутствовать хотя бы одна  $s$ , так как  $Lg = Lh = Lf = Lv = Lu = 0$  – соотношение (3.4). А также если в слове присутствует  $f$  (соответственно,  $v$ ) то должна присутствовать  $g$  (соответственно,  $h$ ), иначе слово можно привести к нулю с помощью  $fh = hf, fv = vf, gv = vg, sf = sv = 0$  – соотношения (3.21), (3.22), (3.11), (3.14). Таким образом, получаем то что требовалось.

(ii) По предложению (3.3.1),  $W = X R^k$ ,  $X$  не содержит  $L$  и  $R$ . Применяя к  $X$  предложение (3.3.4), получаем, что  $W \equiv s^n a^l u^m R^k$  или  $W \equiv s^n b^m t^l g^\alpha h^\beta f^p v^i u^j R^k$ , где  $n, m, l, p, i, j \geq 0, k \geq 1$ , а также  $\alpha, \beta \in \{0, 1\}$ .

В первом случае, если слово содержит  $s$  или  $a$ , то оно приводится к нулю, посредством  $uR = R^2, sR = 0, aR = 0$  – соотношения (3.25), (3.3), (3.5). Если  $s$  и  $a$  нет, слово приводится виду  $R^k$ .

Во втором случае, мы можем применить  $uR = R^2, vR = R^2, fR = R^2$  – соотношения (3.23), (3.24), (3.25) и привести  $W$  к виду  $s^n b^m t^l g^\alpha h^\beta R^k$ , где  $n, m, l \geq 0, k \geq 1$ , кроме того  $\alpha, \beta \in \{0, 1\}$ .

Допустим, что в слове две или более буквы  $R$ .

Тогда, если  $n > 0$  или  $l > 0$ ,  $\alpha = 0$  ( $s$  или  $t$  присутствуют,  $g$  отсутствует), то слово приводится к нулю с помощью  $R^2 = fR$ ,  $fh = hf$ ,  $sf = 0$ ,  $tf = sf = 0$  – соотношения (3.23), (3.21), (3.11).

Аналогично, если  $n > 0$  или  $m > 0$ ,  $\beta = 0$  ( $s$  или  $b$  присутствуют,  $h$  отсутствует), то слово приводится к нулю с помощью  $R^2 = vR$ ,  $vg = gv$ ,  $sv = 0$ ,  $bv = sv = 0$  – соотношения (3.24), (3.22), (3.14).

Таким образом, получаем один из указанных видов.

(iii) По предложению (3.3.1),  $W = L^l X R^k$ ,  $X$  не содержит  $L$  и  $R$ . Применяя к  $W$  первые два утверждения, получаем, что оно имеет следующий вид:

$L^l s^n g^\alpha h^\beta R^m$ , где  $\alpha, \beta \in \{0, 1\}$ , кроме того,  $n, m \geq 1$ .

Если  $m > 1$ , то  $g$  и  $h$  должны присутствовать в слове (аналогично (ii)). Таким образом, получаем то, что требуется.

**Предложение 3.3.6.** В ненулевом слове  $W$  присутствует не более одной буквы  $Q_1$  или  $Q_2$ .

Пусть в слове встретились две или более буквы  $Q_i$ . Тогда в  $W$  существует подслово вида  $Q_i X Q_j$ , где  $X$  не содержит  $Q_1$  и  $Q_2$ . Из предложению (3.3.1) следует, что  $X$  не содержит  $L$  и  $R$ . Согласно предложению (3.3.4),  $X$  представляется в одной из следующих форм:

(i)  $s^n a^m u^j$ ;

(ii)  $s^n b^k t^m g^\alpha h^\beta f^l v^i u^j$ ,

где  $n, k, m, l, i, j \geq 0$ , кроме того  $\alpha, \beta \in \{0, 1\}$ .

Заметим, что  $Q_i a = Q_i u = 0$  и  $bQ_j = tQ_j = gQ_j = hQ_j = fQ_j = vQ_j = uQ_j = 0$  – соотношения (3.7), (3.8). Остается единственная возможность:  $Q_i s^n Q_j$ . Но  $Q_i s = s Q_i$ ,  $Q_i Q_j = 0$  – соотношения (3.17), (3.7).

**Предложение 3.3.7.** Пусть в ненулевом слове  $W$  есть буквы  $Q_i$ ,  $L$ , и как минимум, две  $R$ . Тогда  $W$  может быть представлено в виде:

$L^l a^n s^p Q_i b^k t^m g h R^r$ ,

где  $l, p \geq 1$ ,  $r \geq 2$ ,  $n, k, m \geq 0$ .

Учитывая предложение (3.3.6), в слове только одна  $Q_i$ . Пусть  $W = X_1 Q_i X_2$ . Тогда  $X_1$  содержит  $L$ ,  $X_2$  содержит как минимум, две  $R$  и к этим словам можно применить предложение (3.3.5). Заметим, что

$x Q_i = 0$ , где  $x$  любая буква кроме  $L$ ,  $a$ ,  $s$ ,  $u$  – соотношение (3.7);

$Q_i x = 0$ , где  $x$  любая буква кроме  $b$ ,  $t$ ,  $s$ ,  $g$ ,  $h$ ,  $u$  – соотношение (3.8).

Теперь, перебирая различные варианты – по предложению (3.3.5), получаем, что

Получаем  $W \equiv L^l a^n s^j Q_i s^m b^k t^q g h R^r$ , где  $k, j, n, m, q \geq 0, l \geq 1, r \geq 2$ .

Учитывая, что  $sQ_i = Q_i s$  – соотношение (3.17) получаем требуемый вид.

Упомянутый вид будем считать нормальным видом слова. Таким образом, если в слове присутствуют  $L, Q_i$ , и как минимум, две  $R$ , оно имеет нормальный вид. Посчитаем количество слов, не имеющих нормального вида. Из вышеизложенных лемм следует, что слово, не представляющееся в нормальном виде, может быть представлено одной из следующих форм:

$$\begin{aligned} & s^n a^m u^j; \\ & s^n b^k t^m g^\alpha h^\beta f^l v^i u^j \\ & L^l s^n a^k u^m \\ & L^l s^n g^\alpha h^\beta f^p v^i u^j \\ & s^n b^m t^l g^\alpha h^\beta R \\ & b^m h R^k \\ & t^l g R^k \\ & s^n b^m t^l g h R^k \\ & L^l s^n g h R^k \\ & L^l s^n g^\alpha h^\beta R \\ & L^l a^n s^p Q_i b^k t^m g^\alpha h^\beta R \\ & L^l a^n s^p Q_i b^k t^m g^\alpha h^\beta f^p v^i u^j \end{aligned}$$

Ясно, что общее число слов длины не более  $N$  не имеющих нормальной формы не превосходит  $CN^6$ , где  $C$  – некоторая константа.

### 3.4 Работа основного механизма.

**Предложение 3.4.1.** Пусть  $W = L^l a^n s^p Q_1 b^k t^m g h R^r$ ,

где  $l, p \geq 1, r \geq 2$ , а также  $n, k, m \geq 0$ .

Тогда:

если  $p \leq k$  то  $W \equiv 0$ ;

если  $p > k$ , то  $W \equiv L^l a^{n+k} s^{p-k} Q_i t^{m+k} g h R^r$ .

Допустим,  $p \leq k$ . Применяя  $p$  раз  $Q_1 b s = a Q_1 t$  – соотношение (3.29), получаем  $W \equiv L^l a^{n+p} Q_1 b^{k-p} t^{m+p} g h R^r$ . В данной форме не содержится  $s$ . Применим  $R^2 = u R$  – соотношение (3.26). Учитывая, что  $u$  коммутирует со всеми буквами, кроме  $L, R$  и  $s$  – соотношение (3.16), мы можем

привести слово к виду  $L^l u a^{n+p} Q_1 b^{k-p} t^{m+p} g h R^{r-1}$ . Так как  $Lu = 0$  – соотношение (3.4), получаем  $W \equiv 0$ .

Если  $p > k$ , то применяя  $k$  раз  $Q_1 b s = a Q_1 t$  – соотношение (3.29), получаем требуемое.

**Предложение 3.4.2.** *Пусть  $W = L^l a^n s^p Q_2 b^k t^m g h R^r$ ,*

*где  $l, p \geq 1, r \geq 2, k, n, m \geq 0$ . Тогда*

*если  $p \leq n$  то  $W \equiv 0$ ;*

*если  $p > n$  то  $W \equiv L^l s^{p-n} Q_2 b^{k+n} t^{m+n} g h R^r$*

Допустим,  $p \leq n$ . Применяя  $a Q_2 s = Q_2 b t$  – соотношение (3.27), получаем  $W \equiv L^l a^{n-p} Q_2 b^{k+p} t^{m+p} g h R^r$ . В данной форме не содержится  $s$ . Применим  $R^2 = u R$  – соотношение (3.26). Учитывая, что  $u$  коммутирует со всеми буквами, кроме  $L, R$  и  $s$  – соотношение (3.16), мы можем привести слово к виду  $L^l u a^{n-p} Q_2 b^{k+p} t^{m+p} g h R^{r-1}$ . Так как  $Lu = 0$  – соотношение (3.4), получаем  $W \equiv 0$ .

Если  $p > k$ , применяя  $n$  раз  $a Q_2 s = Q_2 b t$  – соотношение (3.27), получаем требуемое.

**Предложение 3.4.3.** *Пусть  $W = L^l a^n s^p Q_1 t^m g h R^r$ ,*

*где  $l, p \geq 1, r \geq 2, n, m \geq 0$ .*

*Тогда  $W \equiv L^l s^{p-q} Q_j t^{m+q+n} g h R^r$ , где  $q = \frac{(n-1)n}{2}$ .*

Докажем лемму индукцией по  $n$ . При  $n = 0$  она тривиальна, при  $n = 1$  достаточно применить  $th = ht$ ,  $sa = as$ ,  $a Q_1 h = Q_2 th$  – соотношения (3.17), (3.20), (3.28).

Докажем возможность перехода к меньшему  $n$ .

Учитывая  $th = ht$ ,  $sa = as$  – соотношения (3.17), (3.20), получим  $W \equiv L^l s^p a^n Q_1 h t^m g h R^r$ . Теперь применим  $a Q_1 h = Q_2 th$  – соотношение (3.28):  $W \equiv L^l a^{n-1} s^p Q_2 t^{m+1} g h R^r$ . Теперь применяем предложение (3.4.2):

$$W \equiv L^l s^{p-n+1} Q_2 b^{n-1} t^{n+m} g h R^r.$$

Учитывая  $s Q_2 = Q_2 s$ ,  $sb = bs$  – соотношение (3.17):

$$W \equiv L^l Q_2 b^{n-1} s^{p-n+1} t^{n+m} g h R^r.$$

Применяя  $L Q_2 b = L Q_1 t$  – соотношение (3.26), получаем

$$W \equiv L^l s^{p-n+1} Q_1 b^{n-2} t^{n+m+1} g h R^r.$$

Теперь, применяя предложение (3.4.1) получаем

$$W \equiv L^l a^{n-2} s^{p-(n-1)-(n-2)} Q_1 t^{m+(n-1)+(n-2)+2} g h R^r.$$

Для  $n = 2$  формула верна по предположению индукции. Так как  $\frac{(n-3)(n-2)}{2} + n - 1 + n - 2 = \frac{(n-1)n}{2}$ , формула доказана для  $n$ .

**Предложение 3.4.4.** Пусть  $W = L^l a^n s^p Q_2 t^m g h R^r$ ,

где  $l, p \geq 1, r \geq 2, n, m \geq 0$ .

Тогда  $W \equiv L^l s^{p-q} Q_j t^{m+q+n-1} g h R^r$ , где  $q = \frac{(n-1)n}{2} + 1$ .

Фактически это уже было доказано в предложении (3.4.3), после применения первого соотношения.

**Предложение 3.4.5.** Пусть  $W = L^l s^p Q_1 b^k t^m g h R^r$ ,

где  $l, p \geq 1, r \geq 2, k, m \geq 0$ .

Тогда, если  $W \neq 0$ , то  $W \equiv L^l a^{k+1} s^{p+k+1} Q_2 t^{m-k-2} g h R^r$

В дальнейшем будем учитывать, что  $s$  коммутирует с  $Q_i$ , то есть при необходимости мы можем переносить все  $s$  влево или вправо от  $Q_i$ , и кроме того,  $h$  коммутирует с  $t$ , то есть,  $h$  можно переносить влево или вправо от  $t$ .

Применяя  $LQ_1t = LQ_2b$  – соотношение (3.26), затем  $k+1$  раз  $Q_2bt = aQ_2s$  – соотношение (3.27), получаем то, что требуется.

**Предложение 3.4.6.** Пусть  $W = L^l s^p a^k Q_2 t^m g h R^r$ ,

где  $l, p \geq 1, r \geq 2, k, m \geq 0$ .

Тогда, если  $W \neq 0$ , то  $W \equiv L^l s^{p+k+1} a_1^Q b^{k+1} t^{m-k-2} g h R^r$

Применяя  $Q_2th = aQ_1h$  – соотношение (3.28) и затем  $k+1$  раз  $aQ_1t = Q_1bs$  – соотношение (3.29), получаем то, что требуется.

**Предложение 3.4.7.** Пусть  $W = L^l s^p Q_1 t^m g h R^r$ ,

где  $l, p \geq 1, r \geq 2, m \geq 0$ .

Причем  $m$  не может быть представлено ни в одном из видов:  $2n + \frac{(n-1)n}{2}; 2n + \frac{(n-1)n}{2} + 1$  для всех  $n \geq 0$ .

Тогда  $W \equiv 0$ .

Пусть  $m$  не представляется в указанных видах. Тогда  $n \geq 4$ . Возьмем максимальное  $q$ , такое что  $2q + \frac{(q-1)q}{2} < m$ . Будем применять к слову  $W$  поочередно предложения (3.4.5) и (3.4.6). После  $q$  таких применений мы придем к одному из следующих видов, в зависимости от четности  $q$ :

нечетное  $q$ :  $W \equiv L^l a^q s^{p+\frac{(q+1)q}{2}} Q_2 t^{m-2q-\frac{(q-1)q}{2}} g h R^r$

четное  $q$ :  $W \equiv L^l s^{p+\frac{(q+1)q}{2}} Q_1 b^q t^{m-2q-\frac{(q-1)q}{2}} g h R^r$ .

теперь, в случае нечетного  $q$ , применим  $Q_2th = aQ_1h$  – соотношение (3.28) и получим  $W \equiv L^l a^{q+1} s^{p+\frac{(q+1)q}{2}} Q_1 t^{m-2q-\frac{(q-1)q}{2}-1} g h R^r$ . Так как мы

выбрали максимальное  $q$ , имеем  $m - 2q - \frac{(q-1)q}{2} - q - 2 = m - 2(q+1) - \frac{(q+1)q}{2} < 0$  и следовательно  $m - 2q - \frac{(q-1)q}{2} - 1 < q + 1$ . Таким образом, мы можем применить  $m - 2q - \frac{(q-1)q}{2} - 1$  раз  $aQ_1t = Q_1bs$  – соотношение (3.29). Получим слово, не содержащее  $t$ . При этом в слове присутствует как минимум, по одной букве  $a$  и  $b$ . Учитывая, что  $g$  коммутирует с  $b$ , получаем,  $W$  можно привести к виду, содержащему слово  $aQ_1bg$  в качестве подслова. Так как  $aQ_i bg = 0$  – соотношение (3.30) получаем  $W \equiv 0$ .

в случае четного  $q$  применим  $LQ_1t = LQ_2b$  – соотношение (3.26) и получим  $W \equiv L^l s^{p+\frac{(q+1)q}{2}} Q_2 b^{q+1} t^{m-2q-\frac{(q-1)q}{2}-1} ghR^r$ . Теперь применяя  $m - 2q - \frac{(q-1)q}{2} - 1$  раз  $Q_2bt = aQ_2s$  – соотношение (3.27) и Учитывая, что  $g$  коммутирует с  $b$ , получаем,  $W$  можно привести к виду, содержащему слово  $aQ_1bg$  в качестве подслова. Значит,  $W \equiv 0$ .

**Предложение 3.4.8.** Пусть  $W = L^l s^p Q_2 t^m ghR^r$ ,

где  $l, p \geq 1, r \geq 2, m \geq 0$ , причем  $m$  не может быть представлено ни в одном из видов:  $2n + \frac{(n-1)n}{2}$ ;  $2n + \frac{(n-1)n}{2} + 1$  для всех  $n \geq 0$ .

Тогда  $W \equiv 0$ .

Доказательство полностью аналогично доказательству предыдущей леммы, только на этот раз мы начинаем использовать предложения (3.3.2) и (3.3.3) начиная с предложения (3.3.3). Дальнейшее аналогично, с учетом того, что случаи четности  $q$  меняются местами.

Итак, мы доказали, что ненулевое слово содержащее  $L, Q_i$  и две  $R$ , приводится к виду  $L^l s^p Q_i t^m ghR^r$  – предложения (3.3.1)–(3.4.4), причем,  $m$  представляется в виде  $2n + \frac{(n-1)n}{2}$  или  $2n + \frac{(n-1)n}{2} + 1$  – предложения (3.4.5)–(3.4.8).

### 3.5 Система инвариантов.

Теперь приступим к доказательству того, что  $W = L^l s^p Q_i t^m ghR^r$  при  $m = 2n + \frac{(n-1)n}{2} (+1)$  не приводится к нулю, а также единственности этого представления.

Для этого введем систему инвариантов. В этом разделе будем считать, что слово содержит  $L, Q_i$  и как минимум две  $R$ . Из определяющих соотношений следует, что количество  $L, g, h, Q_i$  (без различия индексов) в слове постоянны.

Итак, в нашем слове по одной букве  $g, h, Q_i$ , буквы  $L$  всегда составляют левый префикс, а буквы  $R$  - правый префикс.

Будем говорить, что буква  $x$  *ограничивается* буквами  $(y, z)$ , если любое ненулевое слово, эквивалентное каноническому и содержащее  $x$ , представляется в виде  $AyBxCzD$ , где слова  $B$  и  $C$  не содержат букв  $y$  и  $z$ ,  $A$  не содержит  $x$ ,  $z$  и  $D$  не содержит  $x, y$ .

Заметим, что если буква не ограничена в подслове некоторого слова, то она не ограничена и во всем слове.

Таким образом, из предложения (3.3.1) следует, что любая буква, кроме  $L$  и  $R$  ограничивается  $L$  и  $R$ .

Теперь мы установим ограничивающую пару для каждой буквы и проверим, что свойство букв "быть ограниченной данной парой" не меняется при переходе к эквивалентному слову.

**Ограничение 1.**  $a$  ограничена  $L$  и  $Q_i$ . Количество букв  $L$  и  $Q_i$  в слове не изменяется. Свойство инвариантно относительно всех немономиальных определяющих соотношений (3.16)–(3.29), значит  $a$  ограничена  $L$  и  $Q_i$  в любом слове, эквивалентном  $W$ .

**Ограничение 2.**  $g, h$  ограничены  $Q_i$  и  $R$ . Из определяющих соотношений следует, что в слове всегда присутствует хотя бы одна  $R$  (так как если  $R$  входит в соотношение, то в обе его части), все  $R$  составляют правый префикс слова. Количество букв  $Q_i$  в слове не изменяется. Свойства инвариантны относительно всех немономиальных определяющих соотношений (3.16)–(3.29), значит  $g, h$  ограничены  $Q_i$  и  $R$  в любом слове, эквивалентном  $W$ .

**Ограничение 3.**  $b$  ограничена  $Q_i$  и  $h$ . Количество букв  $h$  и  $Q_i$  в слове не изменяется. Свойство инвариантно относительно всех немономиальных определяющих соотношений (3.16)–(3.29), значит  $b$  ограничена  $Q_i$  и  $h$  в любом слове, эквивалентном  $W$ .

**Ограничение 4.**  $t$  ограничена  $Q_i$  и  $g$ . Количество букв  $g$  и  $Q_i$  в слове не изменяется. Свойство инвариантно относительно всех немономиальных определяющих соотношений (3.16)–(3.29), значит  $t$  ограничена  $Q_i$  и  $g$  в любом слове, эквивалентном  $W$ .

**Ограничение 5.**  $s$  ограничена  $Q_i$  и  $g$  (или  $h$ ). Количество букв  $g, h$  и  $Q_i$  в слове не изменяется. Свойство инвариантно относительно всех немономиальных определяющих соотношений (3.16)–(3.29), значит  $s$  ограничена  $Q_i$  и  $g$  (или  $h$ ) в любом слове, эквивалентном  $W$ .

**Ограничение 6.**  $v$  ограничена  $h$  и  $R$ . Из определяющих соотношений следует, что в слове всегда присутствует хотя бы одна  $R$  (так как если  $R$

входит в соотношение, то в обе его части), все  $R$  составляют правый префикс слова. Количество букв  $h$  в слове не изменяется. Свойство инвариантно относительно всех немономиальных определяющих соотношений (3.16)–(3.29), значит  $v$  ограничена  $h$  и  $R$  в любом слове, эквивалентном  $W$ .

**Ограничение 7.**  $f$  ограничена  $g$  и  $R$ . Из определяющих соотношений следует, что в слове всегда присутствует хотя бы одна  $R$  (так как если  $R$  входит в соотношение, то в обе его части), все  $R$  составляют правый префикс слова. Количество букв  $g$  в слове не изменяется. Свойство инвариантно относительно всех немономиальных определяющих соотношений (3.16)–(3.29), значит  $f$  ограничена  $g$  и  $R$  в любом слове, эквивалентном  $W$ .

Теперь рассмотрим все обнуляющие соотношения и убедимся, что мы не можем привести  $W$  к виду, где встречается левая часть одного из этих соотношений.

Левые части соотношений  $xL = 0, x \neq L; Rx = 0, x \neq R$  (соотношения (3.1), (3.2)) представляют собой слова, где  $x$  не ограничивается  $L$  и  $R$ . Поэтому  $W$  нельзя привести к виду, содержащему одно из этих слов.

Рассмотрим слово  $sR$  – соотношение (3.3). Согласно ограничению 5, любое вхождение  $s$  ограничивается  $L$  и  $g$ . Но  $g$  может встретиться только слева от  $R$ . Получаем, что слово содержащее  $sR$  не удовлетворяет ограничению 5. Поэтому  $W$  нельзя привести к виду, содержащему  $sR$ .

Рассмотрим слово  $Lx$  ( $x \neq L, a, Q_i, s$ ) – соотношение (3.4). Случай  $x = u$  рассмотрим позже. Если  $x = R$ , тогда в слове нет  $Q_i$ , чего быть не может. Если  $x = b, t, g, h$ , то  $x$  не может быть ограничен слева  $Q_i$ . Если  $x = f, v$  то  $x$  не может быть ограничен слева  $g$  и  $h$ . Но в слове эквивалентном  $W$  все эти ограничения присутствуют.

Рассмотрим слово  $ax$  ( $x \neq a, Q_i, s, u$ ) – соотношение (3.5).  $a$  должна быть ограничена справа  $Q_i$ . Тогда если  $x = R$ , то  $R$  не составляют правое окончание слова. Слово  $aL$  уже разбиралось. В остальных случаях,  $x$  ограничен слева  $Q_i$ . Но тогда получается, что в слове присутствует более одной  $Q_i$ , что невозможно.

Рассмотрим слово  $xa$  ( $x \neq L, a, s, u$ ) – соотношение (3.6).  $a$  должна быть ограничена справа  $Q_i$ . Слово  $Ra$  уже разбиралось. В остальных случаях,  $x$  ограничен слева  $Q_i$ , либо  $x = Q_i$ . Но тогда получается, что в слове присутствует более одной  $Q_i$ , что невозможно.

Рассмотрим слово  $xQ_i$  ( $x \neq L, a, s, u$ ) – соотношение (3.7). В случае  $x = R$  получается, что  $R$  не составляют правое окончание слова.

В остальных случаях,  $x$  ограничен слева  $Q_i$ , либо  $x = Q_i$ . Но тогда получается, что в слове присутствует более одной  $Q_i$ , что невозможно.

Рассмотрим слово  $Q_i x$  ( $x \neq b, t, s, g, h, u$ ) – соотношение (3.8). В случае  $x = R, f, v$  получается, что  $g$  или  $h$  (которые обязательно есть в слове), должны входить слева от  $Q_i$ . Но  $g$  и  $h$  сами ограничены  $Q_i$  слева. Значит, в слове присутствует более одной  $Q_i$ , что невозможно.  $x = Q_i, L$  уже разбиралось. Остается  $x = a$ .  $a$  ограничен справа  $Q_i$ . Но тогда получается, что в слове присутствует более одной  $Q_i$ , что невозможно.

Рассмотрим слово  $gx$  ( $x \neq f, b, h, v, R, u$ ) – соотношение (3.9). В случае  $x = t, s, g$  в слове более одной  $g$ , так как  $t, s$  ограничены справа  $g$ .  $x = L, Q_i$  уже разбиралось. Если  $x = a$ , то  $x$  ограничен справа  $Q_i$ ,  $g$  ограничен слева  $Q_i$ . Значит, в слове присутствует более одной  $Q_i$ , что невозможно.

Рассмотрим слово  $fx$  ( $x \neq f, b, h, v, R, u$ ) – соотношение (3.10). Заметим, что  $f$  ограничена слева  $g$ , а значит, и  $Q_i$ . В случае  $x = t, s, g$  в слове более одной  $g$ , так как  $t, s$  ограничены справа  $g$ .  $x = L, Q_i$  уже разбиралось. Если  $x = a$ , то  $x$  ограничен справа  $Q_i$ , Значит, в слове присутствует более одной  $Q_i$ , что невозможно.

Аналогично рассматриваются соотношения (3.11)–(3.15).

Остается два соотношения,  $Lu = 0$  и  $aQ_i bg = 0$ .

Рассмотрим слово  $W = L^l s^p Q_1 t^m g h R^r$  при  $m = 2n + \frac{(n-1)n}{2} (+1)$

Введем функцию  $T(x, y)$ :

$$T(0, 0) = m, T(0, 1) = m - 1,$$

$$T(x, y) = T(x - 1, y + 1) - 1, \text{ если } x + y \text{ нечетное и } T(x - 1, y + 1) > 0;$$

$$T(x, y) = T(x + 1, y - 1) - 1, \text{ если } x + y \text{ четное и } T(x + 1, y - 1) > 0;$$

$$T(x, 0) = T(x - 1, 0) - 1, \text{ если } x \text{ четное и } T(x - 1, 0) > 0;$$

$$T(0, y) = T(0, y - 1) - 1, \text{ если } y \text{ нечетное и } T(0, y - 1) > 0;$$

Теперь докажем, что в слове эквивалентном  $W$  и содержащем соответственно  $n$  и  $k$  букв  $a$  и  $b$ , содержится  $T(n, k)$  букв  $t$ .

**Предложение 3.5.1.** Пусть  $U \equiv W$  и  $U \equiv L^l a^n s^q Q_i b^k t^s g h R^r$ . Тогда  $T(n, k) = s$ .

Заметим, что согласно соотношениям (3.26)–(3.29), сумма вхождений  $a$  и  $b$  в слово меняется тогда и только тогда, когда  $Q_i$  меняет свой индекс.

Допустим, при переходе от  $W$  к эквивалентному слову сумма количества букв  $a$  и  $b$  не изменилась. Если сами числа вхождений при этом изменились, значит применялось  $Q_2 bt = aQ_2 s$  либо  $aQ_1 t = Q_1 bs$  – соот-

ношения (3.27), (3.29). В обоих случаях, согласно определению  $T(x, y)$ , число букв  $t$  изменяется аналогично  $T(x, y)$ .

Пусть теперь сумма количества букв  $a$  и  $b$  ( $n + k$ ) изменилась.

Докажем утверждение при помощи индукции по сумме  $n + k$ . Для  $n + k = 0$  имеем  $T(0, 0) = m$ .

Допустим,  $n + k$  нечетно. тогда у нас в слове –  $Q_2$  и единственным соотношением, увеличивающим  $n + k$  является  $Q_2th = aQ_1h$  – соотношение (3.28). Оно может быть применено, в случае если в слове нет  $b$ . Значит у нас в слове  $n + k$  букв  $a$ , нет букв  $b$  и  $T(n + k, 0)$  букв  $t$ . После применения соотношения в слове  $n + k + 1$  букв  $a$  и  $T(n + k, 0) - 1$  букв  $t$ . Но  $T(n + k + 1; 0) = T(n + k, 0) - 1$ . Индуктивный переход в этом случае завершен.

Случай четной суммы  $n+k$  рассматривается аналогично, только единственным применимым соотношением будет  $LQ_1t = LQ_2b$  – соотношение (3.26).

**Предложение 3.5.2.** (i) Пусть  $T(0, 0) = 2n + \frac{(n-1)n}{2}$ . Тогда

$$T(n, 0) = 0 \text{ при нечетном } n,$$

$$T(0, n) = 0 \text{ при четном } n.$$

(ii) Пусть  $T(0, 0) = 2n + \frac{(n-1)n}{2} + 1$ . Тогда

$$T(n + 1, 0) = 0 \text{ при нечетном } n,$$

$$T(0, n + 1) = 0 \text{ при четном } n.$$

Докажем (i) по индукции. При  $n = 1, 2$  это очевидно. Если это выполнено для нечетного  $n$ , то

$$T(n, 0) = 2(n + 1) + \frac{(n+1)n}{2} - 2n + \frac{(n-1)n}{2} = n + 2$$

Следовательно, по определению  $T(0, n + 1) = T(n + 1, 0) - n - 1 = T(n, 0) - n - 2 = 0$ .

Для четного  $n$  координаты меняются местами.

(ii) Очевидным образом следует из (i) и определения  $T(x, y)$ .

Таким образом, из предложений (3.5.1) и (3.5.2) следует, что если  $W$  приводится к виду, не содержащему букв  $t$ , то либо в слове нет букв  $a$ , либо букв  $b$ . Таким образом, под слово  $aQ_ibg$  встретиться не может.

Теперь допустим, что в слове встретилось  $Lu$ . Это означает, что  $W$  приведено к виду, не содержащему букв  $s$ . Заметим, что путь из состояния  $(0, 0)$  в состояние  $(x, y)$  единственен (мы можем лишь возвращаться по нему назад или идти вперед) и по ходу этого пути количество букв

$s$  не уменьшается. Таким образом, приходим к противоречию с тем, что число букв  $s$  уменьшилось.

Также, учитывая, что применяя соотношения (3.26)–(3.29) мы двигаемся вдоль пути, определенного значениями  $T(x, y)$ , получаем, что представление в точке  $(0, 0)$ , то есть

$$W = L^l s^p Q_1 t^m g h R^r \text{ при } m = 2n + \frac{(n-1)n}{2} (+1) \text{ единственно.}$$

Итак, каждое ненулевое слово, содержащее  $L$ , и две  $R$  приводится к виду  $L^l s^p Q_1 t^m g h R^r$ , где  $m = 2n + \frac{(n-1)n}{2}$  или  $2n + \frac{(n-1)n}{2} + 1$ .

Пусть  $N$  - длина слова. Тогда  $N = l + p + m + r + 3$ . Таким образом, количество таких слов равно  $CN^{3\frac{1}{2}}$ , где  $C$  – некоторая константа.

### 3.6 Преобразование для увеличения количества нормальных слов.

Введем преобразование полугруппы  $S$  в полугруппу  $S^*$ .

Пусть  $S^*$  содержит все буквы и соотношения из  $S$ , кроме того введем еще две дополнительные буквы  $L_1$  и  $R_1$ , а также следующие соотношения:

$$\begin{aligned} xL_1 &= 0 \text{ если } x \neq L_1, \\ L_1x &= 0 \text{ если } x \neq L, L_1, \\ R_1x &= 0 \text{ если } x \neq R_1, \\ yR_1 &= 0 \text{ если } x \text{ или } y \neq R, R_1. \end{aligned}$$

Таким образом, каждому нормальному ненулевому слову  $W$  в полугруппе  $S$  соответствуют ненулевые слова  $L_1^k W R_2^n$  где  $n, k \geq 0$ .

В полугруппе  $S^*$  степень функции роста нормальных слов вида  $L'LXRR'$  увеличивается на 2 по сравнению с функцией роста слов  $LXR$  в полугруппе  $S$ . При этом, степень функции роста слов, не являющихся нормальными увеличивается не более чем на 1.

Таким образом, осуществляя такой переход нужное число раз, мы можем добиться того, что нормальные слова формировали основной член в функции роста полугруппы. Тогда размерность Гельфанд-Кириллова получившейся полугруппы будет нецелой.

## 4. ПОСТРОЕНИЕ ПОЛУГРУППЫ С РЕКУРСИВНОЙ РАЗМЕРНОСТЬЮ ГЕЛЬФАНДА–КИРИЛЛОВА

В настоящей главе будет доказана следующая теорема.

**Теорема 4.0.1.** *Пусть  $\alpha$  – число, для которого существует алгоритм, вычисляющий его двоичные знаки.*

*Тогда для некоторого натурального  $n$  существует конечно-определенная полугруппа с размерностью Гельфанда-Кириллова, равной  $n + \alpha$ .*

### 4.1 План построения полугруппы с рекурсивной размерностью Гельфанда-Кириллова.

В основе построения лежит реализация машины Минского, вычисляющей число  $\alpha$ . Буквы  $Q_i$  играют роль состояний машины Минского. Поскольку машина при вычислении оперирует степенями чисел, необходим механизм, проверяющий что количество вхождений данной буквы есть степень числа. Этот механизм обеспечивается на первом этапе построения. Цель первого этапа – построить полугруппу слов  $S$  в алфавите  $\{L, E, a, g, t, f, u, v, Q_0, \dots, Q_n\}$  с каноническими формами  $L^l a^k E t^{2^k} g Q_0$  и  $L^l a^k E t^m Q_i$  для  $i > 0$ . На втором этапе мы получаем полугруппу слов  $\bar{S}$  в алфавите  $\{R, F, b, h, s, f', u', v', Q_0, \dots, Q_n\}$  с каноническими формами  $Q_n h s^{2^d} F b^d R^r$  и  $Q_i s^{2^z} F b^d R^r$  для  $i < n$ . Вторая полугруппа полностью симметрична первой и получается обращением всех ее определяющих соотношений и последующей заменой букв:

$$L \rightarrow R, E \rightarrow F, a \rightarrow b, g \rightarrow h, t \rightarrow s, f \rightarrow f', u \rightarrow u', v \rightarrow v', Q_0 \rightarrow Q_n$$

При этом буквы  $Q_i$  для  $1 \leq i \leq n$  остаются на месте. На следующем этапе мы рассматриваем полугруппу  $G$ : объединение полугрупп  $S$  и  $\bar{S}$ . При этом произведение любых двух не равных  $Q_i$  букв из разных полугрупп мы принимаем равным нулю. В полугруппе  $G$  канонический вид будет

$$\underline{L^l a^k E t^{2^m} Q_i s^{2^z} F b^d R^r}.$$

Подслово  $E t^{2^m} Q_i s^{2^z} F$  реализует машину Минского. В полугруппе  $G$  мы задаем несколько дополнительных определяющих соотношений, обеспечивающих работу машины. Пусть  $\Gamma$  – конечный граф состояний машины Минского. Вершины этого графа (состояния машины) могут быть соединены одной или несколькими стрелками. Для каждой стрелки мы вводим новую букву  $p_{ij}$ , а также соотношение, соответствующее переходу из одного состояния в другое. При таком переходе рядом с  $Q_i$  будет появляться буква  $p_{ij}$ , соответствующая стрелке сделанного перехода. Основной проблемой которая может появиться при реализации машины Минского является то, что переход по стрелке в полугруппе можно проходить в обе стороны, так как все соотношения двусторонние. При этом, в одну вершину могут входить несколько стрелок. В ситуации, когда рядом с  $Q_i$  появляется буква-идентификатор последнего перехода, вернуться можно только по той стрелке, по которой только что пришли. Таким образом, в этом случае обеспечивается единственность пути преобразований, и этот путь соответствует переходам машины.

С помощью машины Минского мы осуществляем переход  $2^k \rightarrow 2^{[k^\alpha]}$ , где  $[x]$  - целая часть  $x$ . Этому переходу соответствует эквивалентность

$$E t^{2^k} g Q_0 s F \equiv E t Q_n h s^{2^{[k^\alpha]}} F.$$

При этом начальное состояние  $Q_0$  переходит в конечное  $Q_n$ . В полугруппе  $\bar{S}$  согласно каноническому виду при состоянии  $Q_n$  должно быть  $[k^\alpha]$  букв  $b$ . Но количество букв  $b$  неизменно. Самый короткий по длине вид слова, эквивалентного каноническому это  $L^l t a^k g Q_0 h b^{[k^\alpha]} s R^r$ . Количество различных слов такого вида, имеющих длину не более  $N$  равно числу целочисленных решений неравенства  $l + r + k + k^\alpha + 5 \leq N$ , с ограничениями  $l, r, k \geq 1$ .

Далее с помощью конструкции для увеличения количества нормальных слов, описанной в предыдущей главе, мы добиваемся того, что основной член в функции роста обеспечивается словами имеющими канонический вид. Таким образом, получаем размерность Гельфанда–Кириллова, указанную в условии.

Теперь приступим к непосредственной реализации.

В дальнейшем, латинские буквы  $n, k, m, l, d, z$  обозначают целые неотрицательные числа, иногда будет указываться, в каких пределах они

могут изменяться. Греческие буквы  $\gamma, \beta$  обычно равны либо 0 либо 1. Все они будут использоваться для обозначения степеней букв в словах.

#### 4.2 Определяющие соотношения.

Пусть задан алфавит  $\Psi$ :

$$\{L, E, a, g, t, f, u, v, Q_0, \dots, Q_n, 0\}.$$

Рассмотрим полугруппу с нулем  $S$ , порожденную словами в этом алфавите. Нашей целью будет задание конечного числа определяющих соотношений, создающих необходимую нам структуру на полугруппе  $S$ .

Рассмотрим следующее множество соотношений:

$$xL = 0, \quad \text{где } x - \text{любая буква кроме } L; \quad (4.1)$$

$$Q_i x = 0, \quad \text{где } x - \text{любая буква, } i = 0 \dots n; \quad (4.2)$$

$$fx = 0, \quad \text{где } x - \text{любая буква кроме } \{f, Q_0, a\}; \quad (4.3)$$

$$xf = 0, \quad \text{где } x - \text{любая буква кроме } \{f, a, g\}; \quad (4.4)$$

$$gt = gQ_i = gv = 0, \quad \text{где } i = 1 \dots n \quad (4.5)$$

$$gg = 0; \quad (4.6)$$

$$atg = 0; \quad (4.7)$$

$$Lg = 0; \quad (4.8)$$

$$Lttv = 0; \quad (4.9)$$

$$xx = x, \quad \text{где } x = u, v, \text{ или } f, \quad (4.10)$$

$$Q_0 = fQ_0; \quad (4.11)$$

$$ta = att; \quad (4.12)$$

$$ag = ga; \quad (4.13)$$

$$af = fa; \quad (4.14)$$

$$L = LE; \quad (4.15)$$

$$EE = E; \quad (4.16)$$

$$Ea = aE; \quad (4.17)$$

$$xE = 0, \quad \text{где } x - \text{любая буква кроме } \{L, a, E\} \quad (4.18)$$

$$E = Eu; \quad (4.19)$$

$$g = vg; \quad (4.20)$$

$$xy = yx, \quad \text{где } x = u \text{ или } v, y = a \text{ или } t, \quad (4.21)$$

$$xu = 0, \quad \text{где } x - \text{любая буква кроме } \{u, t, a, E, L\}; \quad (4.22)$$

$$vx = 0, \quad \text{где } x - \text{любая буква кроме } \{v, a, t, g\}; \quad (4.23)$$

### 4.3 Приведение к каноническому виду.

Для приведения к каноническому виду нам потребуется несколько лемм.

**Предложение 4.3.1.** *Любое ненулевое слово лексикографически имеет вид  $L^k X Q_i^\beta$ ,*

*где  $X$  не содержит  $L$  и  $Q_i$ ,  $\beta \in \{0, 1\}$ ,  $i \in \{0, \dots, n\}$ ,  $k \geq 0$ .*

*Доказательство.* Если в слове нет букв  $L$  и  $Q_i$ , то оно уже имеет требуемый вид при  $k = \beta = 0$ . Пусть в слове имеется буква  $L$ . Согласно

$xL = 0$ , где  $x \neq L$  – соотношение (4.1), левее  $L$  должны быть тоже  $L$ , таким образом, слово лексикографически имеет вид  $L^nY$ , где слово  $Y$  не содержит  $L$ . Теперь, если в слове есть  $Q_i$ , учитывая  $Q_i x = 0$  – соотношение (4.2), получаем что справа от  $Q_i$  не может быть никаких букв. Таким образом, получаем требуемый вид.  $\square$

**Предложение 4.3.2.** *Пусть  $W$  – некоторое ненулевое слово.*

- (i) *Если  $W$  содержит  $Q_0$ , то  $W$  приводится к виду, не содержащему  $f$ . Если  $W$  содержит  $f$ , но не содержит  $Q_0$ , то  $W$  приводится к виду  $Xf$ , где  $X$  не содержит  $f$ .*
- (ii) *Если  $W$  содержит  $g$ , то  $W$  приводится к виду, не содержащему  $v$ . Если  $W$  содержит  $v$ , но не содержит  $g$ , то  $W$  приводится к виду  $Xv$ , где  $X$  не содержит  $v$ .*
- (iii) *Если  $W$  содержит  $E$  или  $L$ , то  $W$  приводится к виду, не содержащему  $u$ . Если  $W$  содержит  $u$ , но не содержит ни  $L$ , ни  $E$  то  $W$  приводится к виду  $Xu$ , где  $X$  не содержит  $u$ .*

*Доказательство.* (i) Пусть  $W$  не содержит  $Q_0$ , но содержит  $f$ . Выберем крайнее справа вхождение. Слово  $W$  имеет вид  $X_1 f X_2$ , где  $X_2$  не содержит  $f$ . Так как  $W \neq 0$ , то согласно  $fx = 0$ , где  $x \neq f$ ,  $Q_i$ ,  $a$  – соотношение (4.3), первой буквой в слове  $X_2$  может быть только буква  $a$ . (Букв  $Q_0$  и  $f$  слово  $X_2$  не содержит.) Учитывая, что  $fa = af$  – соотношение (4.14),  $f$  можно передвинуть на одну позицию вправо. Далее аналогично получаем, что второй буквой в слове  $X_2$  также является  $a$ . Продолжая аналогично, получим  $X_1 f X_2 \equiv X_1 X_2 f$ . Теперь выберем крайнее справа вхождение  $f$  в слово  $X_1 X_2$ . Повторяя описанные выше рассуждения можно получить вид  $W \equiv X f^m$ , где  $m \geq 1$ . Теперь применяя нужное число раз  $ff = f$  – соотношение (4.10), получаем требуемый вид.

Если  $W$  содержит  $Q_0$ , учитывая предложение (4.3.1), имеем  $W \equiv X Q_0$ , где  $Q_0 \notin X$ . К слову  $X$  применяем рассуждения из первого случая. Получаем  $W \equiv Y f Q_0$ , где  $Q_0, f \notin Y$ . Применяя  $f Q_0 = Q_0$  – соотношение (4.11), получаем вид, не содержащий  $f$ .

(ii) и (iii) рассматриваются аналогично: учитывая соотношения (4.22) и (4.23), получаем, что слева от  $u$  могут находиться только буквы  $u, t, a, E, L$ , а справа от  $v$  только буквы  $v, a, t, g$ . Учитывая, что  $u$  и  $v$  коммутируют с  $a$  и  $t$  – соотношение (4.21), а также  $E = Eu$ ,  $g = vg$  – соотношения (4.19), (4.20), получаем, что требуется.

$\square$

**Предложение 4.3.3.** *Пусть  $W$  – некоторое ненулевое слово.*

*Если  $W$  содержит  $L$ , то  $W$  приводится к виду, не содержащему  $E$ .*

*Если  $W$  содержит  $E$ , но не содержит  $L$ , то  $W$  приводится к виду  $EX$ , где  $X$  не содержит  $E$ .*

*Доказательство.* Пусть  $W$  не содержит  $L$ , но содержит  $E$ . Выберем крайнее слева вхождение. Слово  $W$  имеет вид  $X_1EX_2$ , где  $X_1$  не содержит  $E$ . Так как  $W \neq 0$ , то согласно  $xE = 0$ , где  $x \neq L$ ,  $a$ ,  $E$  – соотношение (4.18), последней буквой в слове  $X_1$  может быть только буква  $a$ . (Букв  $L$  и  $E$  слово  $X_1$  не содержит.) Учитывая, что  $Ea = aE$  – соотношение (4.17),  $E$  можно передвинуть на одну позицию влево. Далее аналогично получаем, что второй справа буквой в слове  $X_1$  также является  $a$ . Продолжая аналогично, получим  $X_1EX_2 \equiv EX_1X_2$ . Теперь выберем крайнее слева вхождение  $E$  в слово  $X_1X_2$ . Повторяя описанные выше рассуждения можно получить вид  $W \equiv E^mX$ , где  $m \geq 1$ . Теперь применяя нужное число раз  $EE = E$  – соотношение (4.16), получаем требуемый вид.

Если  $W$  содержит  $L$ , учитывая предложение (4.3.1), имеем  $W \equiv LX$ , где  $L \notin X$ . К слову  $X$  применяем рассуждения из первого случая. Получаем  $W \equiv LEY$ , где  $L, E \notin Y$ . Применяя  $LE = L$  – соотношение (4.15), получаем вид, не содержащий  $E$ .  $\square$

**Предложение 4.3.4.** *Пусть  $W$  – некоторое ненулевое слово, состоящее из букв  $a, t, g$ , причем  $g$  обязательно содержится в  $W$ .*

*Тогда  $W \equiv a^k t^m g$ , где либо  $m = 2^k$ , либо  $m \geq 2^{k+1}$ .*

*Доказательство.* Учитывая  $gt = 0$  и  $gg = 0$  – соотношения (4.5), (4.6), справа от  $g$  могут быть только  $a$ . Учитывая  $ga = ag$  – соотношение (4.13),  $g$  существует в единственном экземпляре и можно сделать ее крайней справа буквой. Получим  $Ug$ , где  $U$  состоит из  $t$  и  $a$ . Теперь, если в каком-то месте слова встречается подслово  $ta$ , мы заменяем его на подслово  $att$ , используя соотношение (4.12). Повторив эту операцию нужное число раз, получим  $W \equiv a^k t^m g$ .

Допустим,  $m < 2^{k+1}$  и  $m \neq 2^k$ . Тогда  $m = 2^l \times (2p + 1)$ , где  $l < k$ ,  $p \geq 0$ . Из соотношения  $att = ta$  – (4.12), следует, что  $at^{2^s} \equiv t^s a$ . Тогда  $a^{l+1}t^{2^l \times (2p+1)} \equiv t^p ata^l$ . Таким образом, применяя  $ag = ga$  – соотношение (4.13), получаем  $a^k t^m \equiv a^{k-l-1} t^p atga^l$ . Учитывая  $atg = 0$  – соотношение (4.7), получаем  $W \equiv 0$ .  $\square$

**Предложение 4.3.5.** Пусть  $W$  – некоторое ненулевое слово, состоящее из букв  $L, a, t, g, E$  причем  $L$  и  $g$  обязательно содержатся в  $W$ .

Тогда  $W \equiv L^l t a^k g$ , где  $l \geq 1, k \geq 0$ .

*Доказательство.* Учитывая предложения (4.3.1) и (4.3.3), можно считать, что  $W \equiv L^l U$ , где  $L, E \notin U$ .

Допустим, в слове нет букв  $a$ . Учитывая  $gt = 0$  и  $gg = 0$  – соотношения (4.5), (4.6),  $g$  может быть только одна и крайняя справа. Учитывая, что  $Lg = 0$ ,  $g = vg$  и  $Lttv = 0$  – соотношения (4.8), (4.20) и (4.9), получаем  $W = L^l t g$ .

Если в слове нет  $t$ , то его можно привести к нулю с помощью  $ag = ga$  и  $Lg = 0$  – соотношения (4.13), (4.9)

Пусть в слове есть  $a$  и  $t$ . Применяя предложение (4.3.4) к слову  $U$  получаем  $W \equiv L^l a^k t^m g$ , где либо  $m = 2^k$ , либо  $m \geq 2^{k+1}$ . Допустим,  $m \geq 2^{k+1}$ . Тогда применяя  $2^{k+1} - 2$  раза  $att = ta$  – соотношение (4.12), получаем  $W \equiv L^l t t a^k t^{m-2^{k+1}} g$ . Используя  $g = vg$ ,  $va = av$  и  $vt = tv$  – соотношения (4.20) и (4.21), получаем  $W \equiv L^l t t v a^k t^{m-2^{k+1}} g$ . Учитывая  $Lttv = 0$  – соотношение (4.9), получаем  $W \equiv 0$ .

Остается возможность  $m = 2^k$ . В этом случае  $W \equiv L^l t a^k g$ .  $\square$

**Предложение 4.3.6.** Пусть ненулевое слово  $W$  не содержит  $L$  и  $Q_i$ , где  $i = 0 \dots n$ .

Тогда  $W$  представляется в одном из следующих видов:

$a^k f$ ;

$E^\gamma u^\varphi a^k t^m v^\lambda$ , где  $\gamma, \varphi, \lambda \in \{0, 1\}$ ;

$E^\gamma u^\varphi a^k t^m g f^\beta$ , где  $\beta, \gamma \in \{0, 1\}$ ,  $m = 2^k$  или  $m \geq 2^{k+1}$ .

*Доказательство.* Последовательно применяя первую и третью части предложения (4.3.2) (относительно  $f$  и  $u$ ) и предложение (4.3.3), получим, что  $W \equiv E^\gamma u^\varphi X f^\beta$ , где греческие буквы равны 0 или 1,  $X$  не содержит  $E, u, f$ . Значит,  $X$  состоит из букв  $a, t, v, g$ .

Допустим,  $X$  содержит  $g$ . Так как  $gv = gg = gt = 0$  и  $ga = ag$  – соотношения (4.5), (4.6) и (4.13),  $X$  приводится к виду  $Yg$ , где  $Y$  состоит из  $a, t, v$ . Учитывая вторую часть предложения (4.3.2), а также предложение (4.3.4), получаем  $W \equiv E^\gamma u^\varphi a^k t^m g f^\beta$ , где  $m = 2^k$  или  $m \geq 2^{k+1}$ .

Пусть теперь  $X$  не содержит  $g$ . Тогда если  $W$  содержит  $f$ , то  $W \equiv a^k f$ , иначе  $W$  приводится к нулю с помощью  $fa = af$  и  $xf = 0$ , где  $x \neq f, a, g$  – соотношения (4.13) и (4.4). Если  $W$  не содержит  $f$ , то, воспользовавшись второй частью предложения (4.3.2), получаем  $W \equiv$

$E^\gamma u^\varphi Y v^\lambda$ , где  $Y$  состоит из  $a$  и  $t$ . Применив несколько раз  $ta = att$  – соотношение (4.12), получаем  $W \equiv E^\gamma u^\varphi a^k t^m v^\lambda$ .  $\square$

**Предложение 4.3.7.** Любой слово  $W \in S$  может быть приведено либо к нулю, либо к одной из следующих форм:

1.  $a^k f$ ;
2.  $E^\gamma u^\varphi a^k t^m v^\lambda$ ;
3.  $E^\gamma u^\varphi a^k t^m g f^\beta$ , где  $m = 2^k$  или  $m \geq 2^{k+1}$ ;
4.  $L^l a^k t^m v^\lambda$ , где  $l \geq 1$ ;
5.  $L^l a^k t^{2^k} g f^\beta$ , где  $l \geq 1$ ;
6.  $a^k Q_i$ , где  $i = 0 \dots n$ ;
7.  $E^\gamma u^\varphi a^k t^m g Q_0$ , где  $m = 2^k$  или  $m \geq 2^{k+1}$ ;
8.  $E^\gamma u^\varphi a^k t^m Q_i$ , где  $i = 1 \dots n$ ;
9.  $L^l a^k t^{2^k} g Q_0$ , где  $l, k \geq 1$ ;
10.  $L^l a^k t^m Q_i$ , где  $l \geq 1$ .

Примечание: греческие буквы, согласно договоренности, обозначают число, равное 0 или 1.

Девятую форму будем называть первой канонической, десятую – второй канонической. Таким образом, если ненулевое слово содержит  $L$  и  $Q_i$ , то оно приводится к одной из канонических форм.

*Доказательство.* Если  $W$  не содержит  $L$  и  $Q_i$ , имеем условия предложения (4.3.6), и получаем одну из первых трех перечисленных в условии форм.

Если  $W$  содержит  $L$ , но не содержит  $Q_i$ , где  $i = 0 \dots n$  то по предложениям (4.3.1) и (4.3.6) получаем либо  $W \equiv L^l a^k f$ , либо  $W \equiv L^l a^k t^m v^\lambda$  (четвертая форма), либо  $W \equiv L^l a^k t^m g f^\beta$ , где  $\lambda, \beta \in \{0, 1\}$ ,  $m = 2^k$  или  $m \geq 2^{k+1}$ .

$La^k f$  приводится к нулю с помощью  $af = fa$  и  $Lf = 0$  – соотношения (4.14) и (4.4).

Если  $W \equiv L^l a^k t^m g f^\beta$ , тогда  $m < 2^{k+1}$ , иначе слово приводится к нулю с помощью  $att = ta$ ,  $g = vg$ ,  $va = av$ ,  $vt = tv$  и  $Lttv = 0$  – соотношения (4.12), (4.20), (4.21), и (4.9). Но тогда  $m = 2^k$ , так как если  $m$  не делится на  $2^k$ , то слово приводится к нулю с помощью  $att = ta$ ,  $ga = ag$  и  $atg = 0$  – соотношения (4.12), (4.13) и (4.7). Получаем пятую форму из условия предложения.

Таким образом, если  $W$  содержит  $L$ , но не содержит  $Q_i$ , получаем четвертую или пятую из перечисленных в условии форм.

Если  $W$  содержит  $Q_0$ , но не содержит  $L$ , то применяя предложения (4.3.1) и (4.3.6) и, если необходимо,  $fQ_0 = Q_0$  – соотношение (4.11), получаем либо  $a^kQ_0$ , либо  $E^\gamma u^\varphi a^k t^m v^\lambda Q_0$ , либо  $E^\gamma u^\varphi a^k t^m gQ_0$ , где  $t$  делится на  $2^k$ . В первом случае получается шестая форма, в третьем – седьмая, во втором случае слово приводится к нулю с помощью  $Q_0 = fQ_0$  и  $xf = 0$ ,  $x \neq f$ ,  $a, g$  – соотношения (4.11) и (4.4).

Если  $W$  содержит  $Q_i$  ( $i > 0$ ), но не содержит  $L$ , то применяя предложения (4.3.1) и (4.3.6) получаем либо  $a^kQ_i$ , либо  $E^\gamma u^\varphi a^k t^m v^\lambda Q_i$ , либо  $E^\gamma u^\varphi a^k t^m gQ_i$ . В первом случае получается шестая форма, в третьем случае слово приводится к нулю с помощью  $gQ_i = 0$  – соотношение (4.5).

Во втором случае обязательно  $\lambda = 0$ , иначе слово можно привести к нулю с помощью  $vx = 0$ , где  $x \neq v, a, t, g$  – соотношение (4.23). Таким образом, получаем восьмую из перечисленных в условии форм.

Пусть  $W$  содержит  $L$  и  $Q_i$ . Тогда по предложению (4.3.1),  $W = L^l U$ , где  $L \notin U$ . К слову  $U$  можно применить уже разобранный случай, когда в слове содержится  $Q_i$ , но не содержится  $L$  (шестая, седьмая или восьмая формы). Получаем:

$$L^l a^k Q_i, \text{ где } l \geq 1, i = 0 \dots n, \text{ либо}$$

$$L^l E^\gamma u^\varphi a^k t^m gQ_0, \text{ где } t \text{ делится на } 2^k, \text{ либо}$$

$$L E^\gamma u^\varphi a^k t^m Q_i.$$

В первом случае  $i > 0$ , иначе слово приводится к нулю с помощью  $Q_0 = fQ_0$ ,  $fa = af$ ,  $Lf = 0$  – соотношения (4.11), (4.14), (4.4).

Во втором случае с помощью  $L = LE$  и  $E = Eu$  – соотношения (4.19) и (4.15), получаем  $L^l a^k t^m gQ_0$ . Кроме того, если  $t \geq 2^{k+1}$ , с помощью  $ta = att$ ,  $g = vg$ ,  $va = av$ ,  $vt = tv$ , – соотношения (4.12), (4.20), (4.21), слово приводится к виду, содержащему подслово  $Lttv$ , то есть к нулю, согласно соотношению (4.9). Таким образом, получаем  $L^l a^k t^{2^k} gQ_0$  – девятую форму (первую каноническую).

Во втором случае с помощью  $L = LE$  и  $E = Eu$  – соотношения (4.19) и (4.15), получаем  $L^l a^k t^m Q_i$  – десятую форму (вторую каноническую).

□

#### 4.4 Система инвариантов.

Докажем, что канонические слова  $L^l a^k t^m Q_i$ ,  $i > 0$  и  $L^l a^k t^{2^k} gQ_0$  не равны нулю.

Мы используем определение ограниченности, введенное во второй главе.

Будем говорить, что буква  $x$  *ограничивается* буквами  $(y, z)$ , если любое ненулевое слово, эквивалентное каноническому и содержащее  $x$ , представляется в виде  $AyBxCzD$ , где слова  $B$  и  $C$  не содержат букв  $y$  и  $z$ ,  $A$  не содержит  $x$ ,  $z$  и  $D$  не содержит  $x, y$ .

Из определяющих соотношений следуют следующие замечания:

**Замечание 1.** В слове, эквивалентном одному из канонических,  $L$  составляют левый префикс,  $Q_i$  является крайней справа буквой.

**Замечание 2.** В слове, эквивалентном первому каноническому, справа от  $f$  могут встретиться только  $a$  и  $Q_0$ .

**Замечание 3.** В слове, эквивалентном первому каноническому,  $f$  ограничена слева  $g$  и справа  $Q_0$ . В слове, эквивалентном второму каноническому,  $f$  быть не может. ( $f$  может появиться в слове только после применения соотношения  $fQ_0 = Q_0$ , то есть если в слове уже есть  $Q_0$ ).

**Замечание 4.** В слове, эквивалентном первому каноническому,  $t$  ограничена слева  $L$  и справа  $g$ .

**Замечание 5.** В слове, эквивалентном одному из канонических, слева от  $E$  могут встретиться только  $a$ ,  $E$  и  $L$ .

Теперь последовательно переберем все обнуляющие соотношения и убедимся в том, что они не могли встретиться в слове, эквивалентном одному из канонических.

Докажем сначала, что слово из мономиального соотношения не может встретиться в слове, эквивалентном второму каноническому.

Согласно замечанию 3, в слове нет букв  $f$ . Заметим, что букв  $g$  тоже нет, так как если  $g$  есть в левой части определяющего соотношения, то она есть и в правой части. Следовательно, мономиальные соотношения в левой части которых есть буквы  $f$  или  $g$ , встретиться не могут. Также заметим, что слова  $xL = 0$ ,  $x \neq L$  и  $Q_ix = 0$ ,  $x \neq R$ , встретиться не могут, согласно замечанию 1.

Подслово  $xE$ , где  $x \neq L$ ,  $a$ ,  $E$  – соотношение (4.18) встретиться не может, так как согласно ограничению 5, слева от  $E$  может быть лишь  $E$ ,  $a$  или  $L$ .

Остается подслово  $Lttv$  – соотношение (4.9). Заметим, что слово, эквивалентное второму каноническому, не может содержать букву  $g$ , так как эта буква входит либо в обе части определяющего соотношения, либо не входит ни в одну из них. Следовательно, в переходах к эквивалентным словам не участвуют соотношения, содержащие  $g$ . Но тогда, сло-

во, эквивалентное второму каноническому, не может содержать букву  $v$ , эта буква входит либо в обе части определяющего соотношения, не содержащего  $g$ , либо не входит ни в одну из них. Значит, под слово  $Ltv$  встретиться не может.

Итак, ни одно слово из мономиальных соотношений встретиться не могло. Значит, второе каноническое слово не приводится к нулю.

Теперь докажем, что слово из мономиального соотношения не может встретиться в слове, эквивалентном первому каноническому.

Левые части соотношений  $xL = 0$ ,  $x \neq L$ ;  $Q_i x = 0$ ,  $x \neq R$  (соотношения (4.1), (4.2)) представляют собой слова, где нарушается замечание 1. Поэтому  $W$  нельзя привести к виду, содержащему одно из этих слов.

Под слово  $fx$ , где  $x \neq f$ ,  $Q_i$ ,  $a$  – соотношение (4.3) встретиться не может, так как согласно замечанию 2, справа от  $f$  могут быть только  $a$  и  $Q_i$ .

Рассмотрим под слово  $xf$ , где  $x \neq f$ ,  $a$ ,  $g$  – соотношение (4.4). Ясно, что  $x \neq Q_0$ , так как  $Q_0$  всегда правая буква. По замечанию 3,  $f$  ограничена слева  $g$ . Значит, слева от  $x$  встречается  $g$ . Значит  $x \neq L$ . Если  $x = t$ , то так как  $t$  ограничена  $g$  справа, в слове более одной  $t$ , что невозможно. Если  $x = E$ , то слева от  $x$  могут быть только  $a$  и  $L$ , а  $g$  быть не может.

Под слово  $gt$  – соотношение (4.5) встретиться не может, так как согласно замечанию 4, справа от  $t$  должна встретиться  $g$ , тогда в слове более одной  $g$ .

Под слово  $gg$  – соотношение (4.6) встретиться не может, так как тогда в слове более одной  $g$ .

Рассмотрим под слово  $Lg$  – соотношение (4.8). Если в этом же слове есть  $t$ , то справа от этой  $t$  должно быть  $g$ . Тогда в слове более одной  $g$ . Значит в слове отсутствуют буквы  $t$ . Но это невозможно, так как в каноническом слове  $t$  есть и кроме того,  $t$  всегда входит или не входит в обе части определяющего соотношения, поэтому полностью исчезнуть из слова не может.

Под слово  $xE$ , где  $x \neq L$ ,  $a$ ,  $E$  – соотношение (4.18) встретиться не может, так как согласно ограничению 5 слева от  $E$  может быть лишь  $E$ ,  $a$  или  $L$ .

Рассмотрим под слово  $Ltv$  – соотношение (4.9). Определим число  $I(U) = \sum_{j=1}^T 2^{r_j}$ , где  $T$  – количество букв  $t$  в слове,  $r_j$  – количество букв  $a$  находящихся правее от  $j$ -ой по счету буквы  $t$ . Заметим, что величина  $I$  не изменяется при переходе к эквивалентному слову, если это слово не нуль.

Заметим, что количество букв  $a$  остается в слове неизменным. Если слово эквивалентно первому каноническому  $L^l a^k t^{2^k} g Q_0$ , то в нем  $k$  букв  $a$ .

Ясно, что  $I(L^l a^k t^{2^k} g Q_0) = 2^k$ . Для слова  $U$ , содержащего  $Lttv$ , и  $k$  букв  $a$ , получаем  $I(U) \geq 2^k + 2^k = 2^{k+1}$ . Поскольку  $2^k \neq 2^{k+1}$ , заключаем, что  $Lttv$  в нашем слове встретиться не могло.

Рассмотрим слово  $U$ , содержащее  $atg$ . Тогда  $U = U_1 atg U_2$ . Подслово  $U_2$  не содержит букв  $t$ , так как любая  $t$  ограничена  $g$  справа – замечание 4. Пусть в подслово  $U_2$  содержится  $x$  букв  $a$ . Тогда  $x \leq k - 1$  так как во всем слове букв  $a$  ровно  $k$ . Справа от каждой буквы  $t \in U_1$  находится не менее  $x + 1$  букв  $a$ , справа от последней  $t$  ровно  $x$  букв  $a$ . Таким образом,  $I(U)$  не делится на  $2^{x+1}$ , и, так как  $x \leq k - 1$ ,  $I(U)$  не делится на  $2^k$ . Таким образом, слово, содержащее  $atg$ , не может быть эквивалентно первой канонической форме.

Итак, ни одно слово из мономиальных соотношений встретиться не могло. Значит, первое каноническое слово тоже не приводится к нулю.

#### 4.5 Присоединение.

Дополнительно к построенной полугруппе  $S$  нам нужна зеркально симметричная полугруппа  $\bar{S}$ .

Пусть задан алфавит  $\bar{\Psi}$

$$\{R, F, b, h, s, \bar{f}, \bar{u}, \bar{v}, Q_0, \dots, Q_n\}.$$

Определяющие отношения введем следующим образом:

Для каждого определяющего соотношения в полугруппе  $S$  введем соотношение в полугруппе  $\bar{\Psi}$ , получаемое обращением левой и правой частей и заменой букв по следующему правилу:

$$L \rightarrow R, E \rightarrow F, a \rightarrow b, g \rightarrow h, t \rightarrow s, f \rightarrow \bar{f}, u \rightarrow \bar{u}, v \rightarrow \bar{v}, Q_0 \rightarrow Q_n.$$

Буквы  $Q_i$ , где  $1 \leq i \leq n - 1$ , заменяются на себя.

Таким образом, получится полугруппа, слова которой зеркально соответствуют словам полугруппы  $S$  с учетом сделанной замены.

Для получившейся полугруппы  $\bar{S}$  верны все тождества  $S$ , с учетом обратного написания и сделанной замены букв. Канонические слова в  $S$  переходят в канонические слова в  $\bar{S}$ .

Теперь рассмотрим алфавит  $\Psi \bigcup \bar{\Psi}$  – объединение алфавитов полугрупп  $S$  и  $\bar{S}$ .

Будем задавать отношения для конечно-определенной полугруппы  $G$  в этом алфавите.

Возьмем все определяющие соотношения обоих полугрупп, а также добавим соотношения вида  $xy = yx = 0$ , где  $x, y$  любые буквы из  $\Psi \bigcup \bar{\Psi}$  кроме  $Q_i$  для  $i \geq 0$ .

Ненулевые слова из  $G$ , содержащие  $L$  и  $R$ , будем называть каноническими в  $G$ .

Итак, пусть  $W$  – каноническое в  $G$  слово. Если бы  $W$  не содержало  $Q_i$ , то  $W \equiv 0$ , так как произведение любых двух букв, не равных  $Q_i$ , одна из которых принадлежит  $S$ , а другая  $\bar{S}$ , равно нулю. Значит,  $W$  содержит  $Q_i$  и имеет вид  $XQ_iY$ , где  $XQ_i \in S$ ,  $Q_iY \in \bar{S}$ .

Возможны три случая,  $i = 0$ ,  $i = n$ , и  $1 \leq i \leq n - 1$ .

В первом случае, согласно предложению (4.3.7), подслово  $XQ_0$ , содержащее  $L$  и  $Q_0$ , приводится к первой канонической форме в  $S$ , а подслово  $Q_0Y$ , содержащее  $R$  и  $Q_0$ , приводится ко второй канонической форме в  $\bar{S}$ .

Во втором случае, согласно предложению (4.3.7), подслово  $XQ_n$ , содержащее  $L$  и  $Q_n$ , приводится ко второй канонической форме в  $S$ , а подслово  $Q_nY$ , содержащее  $R$  и  $Q_n$ , приводится к первой канонической форме в  $\bar{S}$ .

В третьем случае, согласно предложению (4.3.7), подслово  $XQ_i$ , содержащее  $L$  и  $Q_i$ , где  $1 \leq i \leq n - 1$ , приводится ко второй канонической форме в  $S$ , а подслово  $Q_nY$ , содержащее  $R$  и  $Q_i$ , где  $1 \leq i \leq n - 1$ , приводится ко второй канонической форме в  $\bar{S}$ .

Таким образом, каноническое слово в  $G$  имеет один из следующих видов:

1.  $L^l a^k t^{2^k} g Q_0 s^v b^u R^r$ , где  $l, r, k, v, u \geq 1$ .
2.  $L^l a^k t^m Q_n h s^{2^u} b^u R^r$ , где  $l, r, k, m, u \geq 1$ .
3.  $L^l a^k t^m Q_i s^v b^u R^r$ , где  $l, r, k, v, m, u \geq 1$ ,  $0 < i < n$ .

Во всех трех случаях можно применить  $L = LE$  – соотношение (4.15) в полугруппе  $S$  и зеркальное ему соотношение  $R = FR$  в полугруппе  $\bar{S}$ . Учитывая  $Ea = aE$  – соотношение (4.17) в полугруппе  $S$  и зеркальное ему соотношение  $Fb = bF$ , все три возможных канонических вида приводятся к форме  $L^l a^k M(m, v, i, \beta, \gamma) b^q R^r$ , где  $M(m, p, i, \beta, \gamma) = Et^m g^\beta Q_i h^\gamma s^p F$ ,  $\beta, \gamma = 0$  или 1.

#### 4.6 Создание машины Минского в полугруппе

Итак, мы получили полугруппу  $G$ , такую, что все слова, содержащие буквы  $L$  и  $R$  приводятся к виду  $L^l a^k M(m, v, i, \beta, \gamma) b^u R^r$ , где  $M(m, p, i, \beta, \gamma) = Et^m g^\beta Q_i h^\gamma s^p F$ ,  $\beta, \gamma = 0$  или  $1$ . Кроме того, в главе 1 построена машина Минского  $M$ , вычисляющая  $[K^\alpha]$  универсально по  $K$  для заданного рекурсивного числа  $\alpha$ .

Теперь мы построим полугруппу, реализующую поведение машины Минского.

**Определение 4.6.1.** Инструкцию с номером  $i$  "Добавить в первую ячейку 1 и перейти к инструкции  $j$ " будем обозначать как  $(i, 1, +, j)$

Инструкцию с номером  $i$  "Добавить во вторую ячейку 1 и перейти к инструкции  $j$ " будем обозначать как  $(i, 2, +, j)$

Инструкцию с номером  $i$  "Вычесть из первой ячейки 1 и перейти к инструкции  $j$ , если в первой ячейке нуль, перейти к инструкции  $z$ " будем обозначать как  $(i, 1, -, j, z)$

Инструкцию с номером  $i$  "Вычесть из второй ячейки 1 и перейти к инструкции  $j$ , если во второй ячейке нуль, перейти к инструкции  $z$ " будем обозначать как  $(i, 2, -, j, z)$

В построенной машине Минского  $M$  конечное число состояний  $N$ . Рассмотрим *граф состояний*: вершины графа – это состояния машины Минского, направленное ребро (стрелка) соединяет вершины  $i$  и  $j$ , если инструкция с номером  $i$  включает возможность перехода к инструкции  $j$  (то есть, если  $i$  – инструкция первого рода (прибавляющая единицу), то она должна заканчиваться словами "перейти к  $j$ ", если  $i$  – инструкция второго рода (вычитающая единицу), то она должна включать слова "перейти к  $j$ " либо в случае успешного вычитания, либо в случае, когда вычесть не удалось).

При работе Машина Минского на каждом ходу меняет свое состояние. То есть мы переходим по стрелкам внутри графа состояний. Помимо состояний машины, меняется содержимое ячеек. Переходу от одного состояния Машины Минского к другому соответствует переход от одного слова к другому с помощью некоторого соотношения. Наша цель ввести эти отношения таким образом, чтобы вычислению на машине рекурсивной степени  $\alpha$  (переход  $2^k \rightarrow 2^{k^{\alpha}}$ ) соответствовал переход от слова  $La^k t^{2^k} gQ_0 b^n \rightarrow La^k Q_N h s^{2^{k^{\alpha}}} b^n R$ . В этом случае должно быть выполнено  $n = k^\alpha$ , что вынуждает нужную нам функцию роста слов вида

$Lta^k gQ_0 b^n.$

Для инструкции

i. "Добавить в первую ячейку 1 и перейти к инструкции  $j$ " добавим соотношение  $Q_i = tQ_j$ .

Для инструкции

i. "Добавить во вторую ячейку 1 и перейти к инструкции  $j$ " добавим соотношение  $Q_i = Q_js$ .

Для инструкции

i. "Вычесть из первой ячейки 1 и перейти к инструкции  $j$ , а если в первой ячейке нуль, перейти к инструкции  $z$ " добавим два соотношения:  $tQ_i = Q_j$  и  $EQ_i = Q_z$ .

Для инструкции

i. "Вычесть из второй ячейки 1 и перейти к инструкции  $j$ , а если во второй ячейке нуль, перейти к инструкции  $z$ " добавим два соотношения:  $Q_is = Q_j$  и  $Q_iF = Q_zF$ .

Для перехода от нулевого состояния к первому и от  $n - 1$ -го к  $n$ -му, добавим следующие соотношения:

$$ugQ_0F = Q_1F,$$

$$EQ_{n-1} = EQ_nh\bar{u}.$$

Наличие  $u$  в первом из этих соотношений гарантирует, что в левой части слова остались лишь буквы  $u, t, a, E, L$ , согласно соотношению (4.22). То есть при состоянии Машины Минского, отличном от нуля, в слово не может быть приведено к нулю с помощью соотношения  $Ltv = 0$ , это позволяет изменять количество букв  $t$  в слове, что обеспечивает работу Машины Минского.

Таким образом, список добавленных соотношений такой:

$$xy = yx = 0, \quad \text{где } x \in S, x \in \bar{S}, x, y \neq Q_i; \quad (4.24)$$

$$Q_i = tQ_j, \quad \text{для инструкции } (i, 1, +, j); \quad (4.25)$$

$$Q_i = Q_js, \quad \text{для инструкции } (i, 2, +, j); \quad (4.26)$$

$$tQ_i = Q_j, \quad \text{для инструкции } (i, 1, -, j, z); \quad (4.27)$$

$$EQ_i = EQ_z, \quad \text{для инструкции } (i, 1, -, j, z); \quad (4.28)$$

$$Q_is = Q_j, \quad \text{для инструкции } (i, 2, -, j, z); \quad (4.29)$$

$$Q_iF = Q_zF, \quad \text{для инструкции } (i, 2, -, j, z); \quad (4.30)$$

$$ugQ_0F = Q_1F, \quad (4.31)$$

$$EQ_{n-1} = EQ_nh\bar{u}. \quad (4.32)$$

Идея введения перечисленных соотношений состоит в том, что из заданного слова-состояния Машины Минского можно перейти либо в следующее состояние (применив определяющее соотношение, соответствующее инструкции этого состояния) либо в предыдущее состояние (применив определяющее соотношение, соответствующее инструкции предыдущего состояния, в противоположную сторону). То есть, на графе состояний, из текущей вершины  $i$  можно перейти в вершину, куда ведет исходящая стрелка, либо вернуться в вершину, откуда выходит входящая в  $i$  стрелка.

Заметим, что на графике состояний могут быть циклы. Тогда в одну и ту же вершину могут вести более одной стрелки, то есть добавляется “несанкционированная” возможность перехода назад по стрелке, отличной от той, по которой мы пришли в вершину. Машина начинает свою работу в состоянии  $Q_0$ , в первой ячейке –  $2^k$ , во второй – 0. Для построения критично, чтобы машина не могла вернуться в нулевое состояние с другим значением в первой ячейке. То есть, например, при выполнении перехода  $2^k \rightarrow 3^k 5^k$  (копирование регистра) должна быть обеспечена невозможность возвращения в нулевое состояние со значением в первой ячейке, не равным нулю. Переход  $2^k \rightarrow 3^k 5^k$  реализуется как цепочка переходов  $2^k \rightarrow 2^{k-1} 3 \rightarrow 2^{k-2} 3^2 \rightarrow \dots \rightarrow 3^k 5^k$

При первом переходе этой цепочки делается  $2^{k-1}$  “ходов”, при остальных переходах число ходов делится на три. Организуем график состояний представленный на диаграмме.

Шесть вершин графа, отвечающих состояниям, соединены циклически. Машина ходит по кругу, вычитая по 2 из первой ячейки (и каждый второй ход прибавляя 15 во вторую). Когда в первой ячейке окажется нуль, машина будет находиться в третьем или пятом состоянии, в зависимости от остатка при делении  $k$  на три. Затем происходит переброска содержимого второй ячейки ( $15 \times 2^{k-1}$ ) в первую. После этого машина продолжает движение по циклу. Теперь число ходов до момента, когда в первой ячейке будет нуль, делится на шесть, то есть машина вернется в это же состояние, третье или пятое. Затем повторяется переброска из второй ячейки в первую и так далее. Последний переход начинается со значением в первой ячейке  $3^{k-1} \times 5^{k-1} \times 2$ . При последнем переходе делается  $3^{k-1} \times 5^{k-1}$  ходов (делится на три, но не на шесть), и машина переходит во второе или пятое состояние, далее осуществляется переброска в первую ячейку и выход.

Ясно, что в данном графике состояний вернуться в начальную вершину

можно, только если в первой ячейке –  $2^k$ .

Таким методом (проверяя делимость на соответствующее простое число) организуется невозможность возврата в начальное состояние подпрограммы.

Ясно, что любое слово из полугруппы  $G$  и содержащее  $Q$  имеет вид  $XQ_iY$ , где  $X \in S$ ,  $Y \in \bar{S}$ .

Так как мы собираемся применить конструкцию добавления краев (подробно рассмотренную в предыдущей главе), нам необходимо убедиться, что число слов, не содержащих хотя бы одну из букв  $L$  или  $R$  растет не быстрее некоторого полинома. Это следует из предложения (4.3.7).

В то же время, мы собираемся добиться того, что число слов, содержащих обе буквы  $L$  и  $R$ , выражается как  $\text{const} \times N^{T+\alpha}$ , где  $N$  – длина слова,  $\alpha$  – заданное рекурсивное число,  $T(\alpha)$  – некоторое натуральное число, зависящее от  $\alpha$ .

Если в слове нет  $Q$ , но есть  $L$  и  $R$ , то оно, очевидно, приводится к нулю.

Ясно, что переходя по обратным направлениям стрелок, слово в полугруппе  $G$ , содержащее  $L$ ,  $R$ ,  $Q_i$  приводится либо к нулю, либо к виду, содержащему  $Q_0$ . Но если в слове есть  $Q_0$ , тогда в первой ячейке –  $2^k$ , во второй ячейке – нуль. Таким образом, нужно лишь разобраться со словами  $La^kt^{2^k}gQ_0b^nR$ . Проводя весь цикл работы машины, это слово преобразуется к виду  $La^kQ_ns^{2^{[k^\alpha]}}b^nR$ . То есть, слово не равно нулю, только если  $n = [k^\alpha]$ . Возвращаясь к форме с  $Q_0$ , получаем слово  $La^kt^{2^k}gQ_0b^{k^\alpha}R$ , которое можно записать в виде  $Lta^kgQ_0b^{k^\alpha}R$ . Количество таких слов растет как  $\text{const} \times N^{k+\alpha}$ , где  $N$  – длина слова,  $\alpha$  – заданное рекурсивное число. Окончательно, с помощью конструкции добавления краев, достигаем того, что количество таких слов будет расти быстрее, чем количество слов без какого-то края. Таким образом, получаем, что размерность Гельфанда–Кириллова построенной группы будет равна  $T + \alpha$ , где  $T$  – некоторое натуральное число.

## 5. КОНСТРУКЦИЯ КОНЕЧНО-ОПРЕДЕЛЕННОЙ ПОЛУГРУППЫ, СОДЕРЖАЩЕЙ НЕНИЛЬПОТЕНТНЫЙ НИЛЬ-ИДЕАЛ

На данный момент, вопрос о существовании конечно-определенной ниль-полугруппы является открытым. Тем не менее, оказывается возможным задать с помощью конечного числа определяющих соотношений полугруппу, в которой все слова, содержащие заданную выделенную букву и квадрат некоторого слова, равны нулю.

**Теорема 5.0.1.** *Существует конечно-определенная полугруппа  $H$ , удовлетворяющая следующим свойствам:*

- (i) *Существует ненильпотентный идеал  $I = LH$ , где  $L$  – буква в  $H$ ;*
- (ii) *Если слово  $A \in G$  представляется в виде  $A = XYZ$ , где  $X, Y, Z \in G$ , тогда  $LA = 0$ .*

Пусть задан алфавит  $\Phi$ :

$$\{L, M, P, Q, R, g, s_1, s_2, t_1, t_2, t_3, a_1, a_2, a_3, 0.\}$$

Рассмотрим полугруппу с нулем  $H$ , порожденную словами в этом алфавите. Нашей целью будет задание конечного числа определяющих соотношений, создающих необходимую нам структуру на полугруппе  $H$ .

Рассмотрим следующее множество соотношений:

$$xL = xM = 0, \quad \text{где } x - \text{любая буква из } \Phi; \quad (5.1)$$

$$L = MPg, \quad (5.2)$$

$$ga_i = a_ig, \quad i = 1 \dots 3 \quad (5.3)$$

$$gx = 0, \quad \text{где } x - \text{любая буква из } \Phi \text{ кроме } a_1, a_2, a_3; \quad (5.4)$$

$$a_iga_j = a_iRs_1Qa_j, \quad i, j = 1 \dots 3; \quad (5.5)$$

$$t_i x = xt_i, \text{ где } x \in \{R, a_1, a_2, a_3\}, i = 1 \dots 3; \quad (5.6)$$

$$Pa_it_i = a_iPs_1; \quad (5.7)$$

$$Pa_jt_i = a_jPs_2, \quad i, j = 1 \dots 3, i \neq j; \quad (5.8)$$

$$s_ja_i = a_is_j, \quad i = 1 \dots 3, j = 1, 2; \quad (5.9)$$

$$s_1R = Rs_1; \quad (5.10)$$

$$s_1Qa_i = t_ia_iQ, \quad i = 1 \dots 3; \quad (5.11)$$

$$PRs_1 = 0; \quad (5.12)$$

$$s_2Ra_i = a_is_2R, \quad i = 1 \dots 3; \quad (5.13)$$

$$s_2RQa_i = Rt_ia_iQ, \quad i = 1 \dots 3. \quad (5.14)$$

**Предложение 5.0.1.** *Любое ненулевое слово  $W \in H$ , содержащее  $L$ , лексикографически имеет форму  $W \equiv LA$ , где  $A$  – слово, состоящее из букв  $a_1, a_2, a_3$ .*

*Доказательство.* Пусть  $W$  содержит  $L$ . Учитывая  $xL = 0$ , для любой буквы  $x$  – соотношение (5.1), получаем, что  $L$  может быть только первой буквой в слове  $W$ . Пусть  $W = LU$ . Применяя  $L = MPg$  – соотношение (5.2), получаем  $LU \equiv MPgU$ . Учитывая  $ga_i = a_ig$  и  $gx = 0$  для  $x \neq a_1, a_2, a_3$  – соотношения (5.3) и (5.4) получаем, что если в слове  $U$  встречается любая буква кроме  $a_1, a_2, a_3$ , то  $W$  приводится к нулю.  $\square$

**Предложение 5.0.2.** *Пусть  $X, Y$  некоторые ненулевые слова. Тогда слово  $LXY$  приводится либо к нулю, либо к виду  $MPXRs_1QY$ .*

*Доказательство.* Если  $X$  или  $Y$  содержит какую-либо букву кроме  $a_i$ , то согласно предложению (5.0.1) слово  $LXY$  равно нулю. Пусть  $X$  и  $Y$  состоят из букв  $a_1, a_2, a_3$ . Применяя  $L = MPg$  – соотношение (5.2) получаем  $LXY \equiv MPgXY$ . Далее, применяя (5.3) и (5.5) получаем  $MPgXY \equiv MPXgY \equiv MPXRs_1QY$ .  $\square$

**Предложение 5.0.3.** *Пусть  $U$  – слово состоящее из букв  $a_1, a_2, a_3$ . Тогда  $Pa_iURt_i \equiv a_iPURs_1$ .*

*Кроме того, при  $i \neq j$ ,  $Pa_jURt_i \equiv a_jPURs_2R$ .*

*Доказательство.* Согласно соотношению (5.6)  $Pa_iURt_i \equiv Pa_it_iUR$ . Применяя соотношение (5.7), получаем  $Pa_it_iUR \equiv a_iPs_1UR$ . Учитывая соотношения (5.9) и (5.10), получаем  $a_iPs_1UR \equiv a_iPURs_1$ .

Пусть  $i \neq j$ . Согласно соотношению (5.6)  $Pa_jURt_i \equiv Pa_jt_iUR$ . Применяя соотношение (5.8), получаем  $Pa_jt_iUR \equiv a_jPs_2UR$ . Учитывая соотношение (5.9), получаем  $a_jPs_2UR \equiv a_jPUs_2R$ .  $\square$

**Предложение 5.0.4.** *Пусть  $V$  – слово состоящее из букв  $a_1, a_2, a_3$ . Тогда  $s_1VQa_i \equiv t_iVa_iQ$  и  $s_2RVQa_i \equiv t_iVRa_iQ$ .*

*Доказательство.* Согласно соотношениям (5.9) и (5.10)  $s_1VQa_i \equiv Vs_1Qa_i$ . Применяя соотношение (5.11), получаем  $Vs_1Qa_i \equiv Vt_ia_iQ$ . Учитывая соотношение (5.6), получаем  $Vt_ia_iQ \equiv t_iVa_iQ$ .

Согласно соотношению (5.13)  $s_2RVQa_i \equiv Vs_2RQa_i$ . Применяя соотношение (5.14), получаем  $Vs_2RQa_i \equiv VRt_ia_iQ$ . Применяя соотношение (5.6), получаем  $VRt_ia_iQ \equiv t_iVRa_iQ$ .  $\square$

**Предложение 5.0.5.** *Пусть  $X, VZ$  – слова состоящее из букв  $a_1, a_2, a_3$ . Тогда  $PXVRZs_1QX \equiv XPVRs_1ZXQ$  и  $PXs_2VRQX \equiv XPVRs_1XQ \equiv 0$ .*

*Доказательство.* Докажем первую эквивалентность индукцией по длине  $X$ . Для  $X = a_i$  все следует из предложений (5.0.3) и (5.0.4). Пусть  $X = a_iU$ , то есть  $a_i$  – первая буква  $X$ . По предложению (5.0.4),  $PXVRZs_1QX = PXVRZs_1Qa_iU \equiv PXVRZt_ia_iQU$ . Применяя (5.6), получаем  $PXVRZt_ia_iQU \equiv PXVRt_iZa_iQU$ . По предложению (5.0.3),  $PXVRt_iZa_iQU = Pa_iUVRt_iZa_iQU \equiv a_iPUVRs_1Za_iQU \equiv a_iPUVRZa_is_1QU$ . Таким образом, можно рассматривать слово  $PUVRZa_is_1QU$ , для которого верно предположение индукции.

Вторая эквивалентность аналогична первой, только на первом этапе используется вторая часть предложения (5.0.4).  $\square$

**Предложение 5.0.6.** *Пусть  $i, j, k \in \{1 \dots 3\}$  и  $i \neq j$ . Тогда  $Pga_ia_ja_k = a_iPga_ja_k$ .*

*Доказательство.* Учитывая соотношения (5.3) и (5.5), получим  $Pga_ia_ja_k \equiv Pa_iRs_1Qa_ja_k$ . По соотношению (5.11),  $Pa_iRs_1Qa_ja_k \equiv Pa_iRt_ja_jQa_k$ . Далее, по соотношениям (5.6) и (5.6),  $Pa_iRt_ja_jQa_k \equiv Pa_it_jRa_jQa_k \equiv a_iPs_2Ra_jQa_k$ . По соотношению (5.13),  $a_iPs_2Ra_jQa_k \equiv a_iPa_js_2RQa_k$  и, по соотношению (5.14),  $a_iPa_js_2RQa_k \equiv a_iPa_jRt_ka_kQ$ . Теперь, применяя соотношение (5.5), получаем  $a_iPa_jRt_ka_kQ \equiv a_iPa_jga_k$ . Применяя  $ga_j = a_jg$ , получаем требуемое.  $\square$

**Предложение 5.0.7.** *Пусть  $X, Y, Z$  – непустые слова. Тогда  $LXYZ \equiv 0$ .*

*Доказательство.* Учитывая предложение (5.0.1), можно считать, что  $X, Y, Z$  – слова состоящие из букв  $a_1, a_2, a_3$ .

Применим соотношение (5.1)  $LXYZ \equiv MPgXYZ$ . Применяя предложение (5.0.6) нужное число раз, получаем  $MPgXYZ \equiv MXPgYZ$ .

Далее рассмотрим подслово  $PgYY$ . Учитывая (5.0.2), Получаем  $PgYY \equiv PYRs_1QY$ . Теперь по предложению (5.0.5) (с пустыми словами  $V$  и  $Z$ ) и соотношению (5.12), получаем  $PYRs_1QY \equiv YPRs_1YQ \equiv 0$ .

□

**Предложение 5.0.8.** *Пусть ненулевое слово  $W$  содержит букву  $L$ . Тогда для любого слова  $U$ , эквивалентного  $W$ , возможен один из трех случаев:*

- (i) Слово  $U$  имеет вид  $LA$ , где  $A$  – слово состоящее из букв  $a_1, a_2, a_3$ ;
- (ii) Слово  $U$  имеет вид  $MA_1PA_2gA_3$ , где  $A_1, A_2, A_3$  – слова, состоящие из букв  $a_1, a_2, a_3$ ;
- (iii) В слове  $U$  нет букв  $L$  и  $g$ , при этом  $U$  содержит одну букву (первую)  $M$ , одну букву  $P$ , одну  $R$ , одну  $Q$  и одну букву из множества  $\{t_1, t_2, t_3, s_1, s_2\}$ . При этом, буквы  $P, Q, R$  входят именно в таком порядке.

*Доказательство.* Для каждого ненулевого слова  $W$  введем следующие обозначения:

$I_0(W)$  – суммарное количество букв  $L$  и  $M$  в слове.

$I_1(W)$  – суммарное количество букв  $L$  и  $P$  в слове.

$I_2(W)$  – суммарное количество в слове букв  $L, g, R$ .

$I_3(W)$  – суммарное количество в слове букв  $L, g, Q$ .

$I_4(W)$  – суммарное количество в слове букв  $L, g, t_1, t_2, t_3, s_1, s_2$ .

Заметим, что числа  $I_0, I_1, I_2, I_3, I_4$  одинаковы для левой и правой части любого определяющего соотношения. Следовательно, эти числа не меняются при переходе к эквивалентному слову, то есть являются инвариантами. По предложению (5.0.1),  $W$  может быть приведено к виду  $LA$ , где  $A$  – произведение букв  $a_1, a_2, a_3$ . Заметим, что  $I_0(LA) = I_1(LA) = I_2(LA) = I_3(LA) = I_4(LA) = 1$ . Следовательно, для ненулевого слова все четыре инварианта равны единице.

Если в слове присутствует буква  $L$ , то согласно предложению (5.0.1) букв  $P, g, R, Q, t_1, t_2, t_3, s_1, s_2$  в нем нет. В этом случае реализуется первый случай из условия настоящего предложения.

Если в слове нет буквы  $L$ , то в нем есть ровно одна буква  $M$  ( $I_0 = 1$ ), причем она может быть только первой слева, так как есть только одно немономиальное соотношение с участием  $L$  и  $M$  и это  $L = MPg$ . Кроме того, в слове только одна  $P$ , так как  $I_1 = 1$ . Рассмотрим два случая.

Пусть в слове есть буква  $g$ . Тогда она ровно одна, и в слове нет букв  $R, Q, t_1, t_2, t_3, s_1, s_2$  так как  $I_2 = I_3 = I_4 = 1$ . Таким образом, слово имеет вид  $MA_1PA_2gA_3$ , где  $A_1, A_2, A_3$  – слова содержащие только буквы  $a_1, a_2, a_3$ .

Пусть теперь в слове нет буквы  $g$ . Так как  $I_1 = I_2 = I_3 = I_4 = 1$ , то в слове одна буква  $P$ , одна  $R$ , одна  $Q$  и одна буква из множества  $\{t_1, t_2, t_3, s_1, s_2\}$ . Окончательно заметим, что по предложению (5.0.1) все слова могут быть приведены к виду  $LA$ , и из этого вида можно получить вид содержащий буквы  $P, Q, R$  в данном порядке. Кроме того, никакое определяющее соотношение не может поменять этот порядок. Таким образом, получаем третий случай из перечисленных в условии предложения.  $\square$

**Предложение 5.0.9.** *Пусть  $U$  – слово, состоящие из букв  $a_1, a_2, a_3$ , не содержащее двух одинаковых подслов, идущих подряд. Тогда  $LU \neq 0$ .*

*Доказательство.* Допустим,  $LU \equiv 0$ . Тогда существует цепочка эквивалентных слов, начинающаяся с  $LU$  и заканчивающаяся нулем. Каждый переход в этой цепочке использует какое-либо определяющее соотношение. Последним переходом является одно из четырех соотношений:  $xL = 0, gx = 0, t_i a_j Q = 0, PRs_1 = 0$ . Последовательно разберем каждое из них и убедимся, что ни одно из них встретиться не может.

$xL = 0$  встретиться не может, так как если буква  $L$  присутствует в слове, то она является крайней слева (а если отсутствует, то крайней слева является  $M$ ).

$gx = 0$  не может встретиться, так как если в слове есть  $g$ , то оно по предложению (5.0.8) будет иметь вид  $MA_1PA_2gA_3$ , где в слове  $A_3$  нет букв, отличных от  $a_1, a_2, a_3$ .

Рассмотрим соотношение  $t_i a_j Q = 0$ . Заметим, что в любом слове, эквивалентном  $LA$  (где  $A$  состоит лишь из букв  $a_1, a_2, a_3$ ) выполнено следующее свойство: если  $s_1$  входит в слово, то последняя буква  $a$  из подслова между  $R$  и  $Q$  совпадает с буквой, ближайшей слева к  $P$ . Действительно, сначала в слове нет  $Q$ . Появиться она может лишь с помощью соотно-

шения (5.5):  $a_i g a_j = a_i R s_1 Q a_j$ . То есть, пока между  $R$  и  $Q$  нет букв  $a$ . Пусть мы перешли к какому-либо эквивалентному слову, в котором тоже есть  $s_1$ . Легко видеть, что при этом переходе нам пришлось бы воспользоваться соотношениями  $P a_i t_i = a_i P s_1$  и  $s_1 Q a_i = t_i a_i Q$  в чередующемся порядке и равное число раз. (Аналогично с соотношениями  $P a_j t_i = a_j P s_2$  и  $s_2 R Q a_i = R t_i a_i Q$ ). Ясно, что при этом последняя буква  $a$  из под слова между  $R$  и  $Q$  совпадет с буквой, ближайшей слева к  $P$ . Таким образом, если в  $s_1$  входит в слово, то последняя буква  $a$  из под слова между  $R$  и  $Q$  совпадает с буквой, ближайшей слева к  $P$ .

Итак, допустим, есть слово  $M A_0 P A_1 R A_2 t_i a_j Q A_3$ .

Рассмотрим соотношение  $P R s_1 = 0$ . Предположим, что существует цепочка эквивалентных переходов, ведущая от слова  $A_0 P A_1 R s_1 Q A_2$  к слову  $B_0 P R s_1 B_1 Q B_2$ , где слова  $A_i, B_i$  состоят из букв  $a_1, a_2, a_3$ , причем  $A_0 A_1 A_2 = B_0 B_1 B_2$  – лексикографическое равенство. Будем называть *расстоянием между буквами  $X$  и  $Y$*  количество букв  $a_1, a_2, a_3$ , находящихся между  $X$  и  $Y$ . Обозначим расстояние как  $d(X, Y)$ . Заметим, что величина " $d(P, Q) +$  количество букв  $s_1$  или  $s_2$  в слове" является инвариантом в данной цепочке эквивалентных переходов (в данных переходах не участвуют слова, содержащие  $g$ ). Кроме того, заметим, что при эквивалентном переходе из букв  $s_1$  и  $s_2$  получается одна из трех букв  $t_1, t_2, t_3$ , а из буквы  $t_i$  – буква  $s_1$  или  $s_2$ . Таким образом, слова в основной цепочке эквивалентности можно разбить на чередующиеся группы, так что в одной группе все слова содержат  $t_i$ , в следующей –  $s_1$  или  $s_2$ , и так далее. Рассмотрим перехода, когда мы выходим из цепочки, то есть в результате которого получается первое слово следующей цепочки. После этого перехода во всех словах в качестве  $s_i$  входит  $s_1$ . Поскольку этот переход заканчивает цепочку, в нем используются соотношения, содержащие  $s_2$  только с одной стороны. То есть  $s_2$  превращается в одну из трех букв  $t_1, t_2, t_3$ . Таких соотношений всего два:  $a_j P s_2 = P a_j t_i$  и  $s_2 R Q a_i = R t_i a_i Q$ .

Допустим переход, выводящий из цепочки, где все слова содержат  $s_2$ , произошел с помощью соотношения  $a_j P s_2 = P a_j t_i$ . Таким образом, первое слово следующей цепочки (все слова которой содержат  $t_i$ ) имеет вид  $A_0 P a_j t_i A_1 R A_2 Q A_3$ . Так как мы выбирали последнюю цепочку с  $s_2$ , все последующие цепочки характеризуются либо  $s_1$ , либо  $t_i$ . То есть все последующие переходы между цепочками реализуются с помощью соотношений  $s_1 Q a_i = t_i a_i Q$  и  $P a_i t_i = a_i P s_1$ . При этом легко заметить, что применяя эти соотношения, к слову  $A_0 P a_j t_i A_1 R A_2 Q A_3$  расстояние между  $P$  и  $R$  меньше сделать нельзя, так как  $j \neq i$ .

Пусть теперь переход, выводящий из цепочки, произошел с помощью соотношения  $s_2RQa_i = Rt_ia_iQ$ . Тогда, первое слово следующей цепочки (все слова которой содержат  $t_i$ ) имеет вид  $A_0PA_1Rt_ia_iQA_3$ . Поскольку в дальнейшем, определяющие соотношения, содержащие  $s_2$  не применяются, все последующие переходы между цепочками реализуются с помощью соотношений  $s_1Qa_i = t_ia_iQ$  и  $Pa_it_i = a_iPs_1$ . Тогда в дальнейшем действует следующее правило: если в слове есть  $s_1$ , то ближайшие к  $P$  и  $Q$  слева буквы  $a_i$  одинаковы, и если в слове есть  $t_j$ , то ближайшие к  $Q$  слева буква (из  $a_1, a_2, a_3$ ) равна  $a_j$ . Кроме того, заметим, что  $R$  не меняет своего положения внутри слова. Итак, пусть в какой-то момент мы получили подслово  $PRs_1$ . Тогда, согласно вышеизложенному, мы перешли от слова  $A_0PA_1Rt_ia_iQA_3$  к слову  $A_0A_1PRs_1a_i\widetilde{A_3}QA_4$ . При этом при каждом шаге вправо слева от  $P$  и  $Q$  оставалась одна и та же буква  $a_i$ . Таким образом, слова  $A_1$  и  $a_i\widetilde{A_3}$  лексикографически равны, то есть изначально слово из букв  $a_1, a_2, a_3$  содержало два одинаковых подслова, идущих подряд. Таким образом получили противоречие.

Таким образом, ни одно из слов, равных нулю, получить нельзя.

□

## БИБЛИОГРАФИЯ

- [1] Krause G. R., Lenagan T. H. Growth of algebras and Gelfand-Kirillov dimension. London: Pitman Adv. Publ. Program, 1985, 182.
- [2] Belov A. J., Borisenko V. V., Latysev V. N. Monomial Algebras. NY. Plenum, 1997.
- [3] Уфнаровский В. А. О росте алгебр. Вестник МГУ. вып 1, 1978, 4, 59–65.
- [4] Gelfand I. M., Kirillov A. A. Sur les corps liés aux algébras enveloppantes des algébras de Lie. Publs. math. Inst. hautes étud. sci., 1966, 31, 509–523.
- [5] Sapir M. V. Algorithmic Problems for Amalgams of Finite Semigroups.
- [6] Latyshev V. On the recognizable properties of associative algebras. Special vol. J.S.C.: On computational aspects of commutative algebras. London: Acad. Press, 1988, 237–254.
- [7] Kukin G. P. The variety of all rings has Higman's property. Algebra and Analysis. Irkutsk. 1989 91–101
- [8] Bokut L. A., Kukin G. P. Algorithmic and combinatorial algebra. Math. and its appl. 233.
- [9] Belyaev V. Ya. Imbeddability of recursively defined inverse semigroups in finitely presented semigroups. Sibirsk. Math. Journal 25 no. 2., 1984. 50–54.
- [10] Belov A. Ya. Ivanov I. A Construction of Semigroups with Some Exotic Properties, Comm. in Algebra, Volume 31, Number 2, 2003. 673–696.
- [11] Belov A. Ya. Ivanov I. A Construction of Semigroups with Some Exotic Properties, Acta Appl. Math 85 (2005), no 1-3, 49–56.
- [12] Bergman G. The diamond lemma for ring theory. Adv. Math., 1978, 29, 2, 178–218.

- [13] Иыуду Н. К. Алгоритмическая разрешимость проблемы распознавания делителей нуля в одном классе алгебр. Фунд. и прикл. матем., 1995, 2, 1, 541–544.
- [14] Иыуду Н. К. Стандартные базисы и распознаваемость свойств алгебр, заданных копредставлением. Дисс. на соиск. уч. ст. канд. физ. мат. наук — Москва, 1996, 73.
- [15] Пионтковский Д. И. Базис Грёбнера и когерентность мономиальной ассоциативной алгебры. Фунд. и прикл. матем., 1996, 2, 2, 501–509.
- [16] Пионтковский Д. И. Некоммутативные базисы Грёбнера, когерентность ассоциативных алгебр и делимость в полугруппах. Фунд. и прикл. матем., 2001, 7, 2, 495–513.
- [17] Белов А. Я. Линейные рекуррентные уравнения на дереве. Математические заметки, 78, N5, 643–651.
- [18] Уфнаровский В. А. Комбинаторные и асимптотические методы в алгебре. Итоги науки и техн. Сер. Соврем. probl. мат. Фундам. направления. — М.: ВИНИТИ, 1990, 57, 5–177.
- [19] И. А. Иванов-Погодаев, "Алгебра с конечным базисом Грёбнера, и неразрешимой проблемой делителей нуля", Фундаментальная и прикладная математика, том 12(4), 2006.
- [20] Zelmanov E. On the nilpotency of nilalgebras. Lect. Notes Math., 1988, 1352, 227–240. РЖМат, 1989, 7A188)
- [21] Ширшов А. И. О некоторых неассоциативных ниль-кольцах и алгебраических алгебрах. Мат. сб., 1957, 41, 3, 381–394. (РЖМат, 1958, 164)
- [22] Ширшов А. И. О кольцах с тождественными соотношениями. Мат. сб., 1957, 43, 2, 277–283. РЖМат, 1958, 7544)
- [23] Днестровская тетрадь: оперативно-информац. сборник — 4-е изд. — Новосибирск: изд. ин–та матем. СО АН СССР, 1993, 73.
- [24] Кострикин А. И. Вокруг Бернсайда. — М.: Наука, 1986, 232.