Проконечные группы, ассоциированные со слабо примитивными подстановками

Ж. АЛМЕЙДА
Университет Порту, Португалия
e-mail: jalmeida@fc.up.pt

УДК 512.53

Ключевые слова: свободная проконечная полугруппа, проконечная группа, символическая динамика, итерированная подстановка.

Аннотация

Вполне рекуррентное псевдослово — это элемент свободной проконечной полугруппы, в котором каждое конечное подслово появляется в каждом достаточно длинном конечном подслове. По-другому его можно охарактеризовать как псевдослово, которое является подсловом всех своих бесконечных подслов, т. е. которое лежит в таком $\mathcal{J}$-классе, что лишь конечные слова могут быть строго $\mathcal{J}$-выше его. Такой $\mathcal{J}$-класс регулярен и, следовательно, с ним ассоциирована некоторая проконечная группа, а именно любая из его максимальных подгрупп. Одним из способов получить такой $\mathcal{J}$-класс является итерирование конечных слабо примитивных подстановок. Настоящая работа посвящена вычислению проконечной группы, ассоциированной с $\mathcal{J}$-классом, порождённым бесконечной итерацией конечной слабо примитивной подстановки. Основной результат заключается в том, что эта группа является свободной проконечной группой при условии, что обратима подстановка, индуцированная свободной группой на буквах, которые появляются в образах всех их достаточно длинных итераций.

Abstract

J. Almeida, Profinite groups associated with weakly primitive substitutions, Fundamentalnaya i prikladnaya matematika, vol. 11 (2005), no. 3, pp. 13—48.

A uniformly recurrent pseudoword is an element of a free profinite semigroup in which every finite factor appears in every sufficiently long finite factor. An alternative characterization is as a pseudoword that is a factor of all its infinite factors, i.e., one that lies in a $\mathcal{J}$-class with only finite words strictly $\mathcal{J}$-above it. Such a $\mathcal{J}$-class is regular, and therefore it has an associated profinite group, namely any of its maximal subgroups. One way to produce such $\mathcal{J}$-classes is to iterate finite weakly primitive substitutions. This paper is a contribution to the computation of the profinite group associated with the $\mathcal{J}$-class that is generated by the infinite iteration of a finite weakly primitive substitution. The main result implies that the group is a free profinite group provided the substitution induced on the free group on the letters that appear in the images of all of its sufficiently long iterates is invertible.

Фундаментальная и прикладная математика, 2005, том 11, № 3, с. 13—48.

1. Введение

Теория проконечных полугрупп, в частности являющихся свободными относительно псевдомногообразий, начала привлекать значительное внимание с середины 1980-х гг. Основной интерес к этой теории вызван её связью с теорией языков и автоматов через соответствие Эйленберга между некоторыми классами рациональных языков и псевдомногообразиями полугрупп. В частности, структурные результаты, касающиеся относительно свободных проконечных полугрупп, часто могут привести к важным приложениям [2, 4, 5, 10, 11, 23]. Однако до сих пор очень мало известно о структуре абсолютно свободных проконечных полугрупп, элементы которых называют *псевдословами*. В этой статье продолжается изучение связи между структурой конечно порождённых свободных проконечных полугрупп и символической динамикой, которая впервые была выявлена в [3] и была также использована в [10].

Одна из ключевых идей подхода, использующего символическую динамику, заключается в том, чтобы получать псевдослова, итерируя эндоморфизмы свободной проконечной полугруппы. Возможность таких итераций обоснована результатом, утверждающим, что если проконечная полугруппа конечно порождённая, то её моноид непрерывных эндоморфизмов сам является проконечным моноидом относительно топологии поточечной сходимости [5]. Таким образом, можно естественно определить бесконечную итерацию непрерывного эндоморфизма, а именно ту единственную итерацию, которая является идемпотентом, (её называют *ω-степенью* эндоморфизма). Эта техника была использована в [3], для того чтобы показать, что псевдомногообразие конечных p-групп является ручным (см. [4, 8, 9] о значении этого свойства), и в [10], чтобы построить множество псевдослов, которые затем могут быть использованы для изучения псевдомногообразий, подгруппы элементов которых лежат в данном псевдомногообразии групп.

Идея, разрабатываемая в данной работе, состоит в том, чтобы итерировать конечные подстановки для получения феномена равномерной рекуррентности. Эта статья — вклад в понимание устройства $\mathcal{J}$-классов равномерно рекуррентных псевдослов. В разделе 2 мы покажем, что $\mathcal{J}$-классы, целиком состоящие из равномерно рекуррентных псевдослов, это в точности те $\mathcal{J}$-классы, $\mathcal{J}$-выше которых лежат лишь конечные слова, и поэтому эти классы регулярны. Развивая далее связь с символической динамикой (что однако выходит за рамки данной работы, см. [6, 7]), можно показать, что имеется взаимно-однозначное соответствие с минимальными символическими динамическими системами, устанавливаемое с помощью языка конечных подслов.

В частности, с каждым равномерно рекуррентным псевдословом мы свяжем проконечную группу, взяв любую из максимальных подгрупп в $\mathcal{J}$-классе этого псевдослова (хорошо известно, что все они изоморфны). В разделах 3—5 разрабатывается метод, который в достаточно широком классе случаев позволит вычислить такие проконечные группы. Основным результатом статьи является теорема 5.3, утверждение которой носит слишком технический характер,

чтобы воспроизводить её здесь. Зато широкий класс приложений обеспечивает следствие 5.7, в котором устанавливается, что если конечная слабо примитивная подстановка действует как автоморфизм на свободной группе, порождённой множеством слов, являющихся образами бесконечных итераций этой подстановки, то соответствующая проконечная группа является конечно порождённой свободной. Кроме того, теорема 5.3 даёт способ явно выписать свободные порождающие этой проконечной группы.

В разделе 6 показано, что внутри нашего широкого класса равномерно рекуррентных $\mathcal{J}$-классов можно найти $\mathcal{J}$-классы Штурма и Арну—Рози, связанные соответственно с символическими динамическими системами Штурма и Арну—Рози, порождёнными подстановками (более подробную информацию об этих системах можно найти в [14, 18]). В этом случае рассматриваемые группы являются n-порождёнными свободными проконечными группами, если система содержит в точности n букв. Обобщение этого результата на системы, не обязательно порождённые подстановками, было анонсировано в [7].

Наконец, в разделе 7 представлены несколько примеров, в том числе пример максимальной полугруппы равномерно рекуррентных $\mathcal{J}$-классов, которая не является свободной проконечной группой.

Решающую роль при доказательстве результатов данной статьи сыграл комбинаторный инструментарий: элементарная комбинаторная теория групп вместе с некоторыми разделами алгебраической теории кодов, а именно циклических кодов и кодов с ограниченным запаздыванием. Все необходимые вспомогательные результаты приведены с доказательствами, что делает настоящую работу замкнутой в этом отношении. Мы также будем использовать некоторые важные теоремы теории кодирования из [15, 19].

Предварительные версии основных результатов этой статьи анонсировались автором на различных встречах и семинарах. Также они были анонсированы без доказательств в [6, 7].

2. Равномерная рекуррентность как алгебраическое свойство

Всюду в этой статье через A обозначается конечное множество, называемое *алфавитом*, A^* — свободный моноид над A.

Напомним, что *проконечный моноид* — это компактный нульмерный моноид, или, эквивалентно, проективный предел конечных моноидов, рассматриваемых как топологические моноиды в дискретной топологии. Обозначим через $\widehat{A^*}$ *свободный проконечный моноид*, полученный как проконечное пополнение свободного моноида A^* [5]. *Псевдословами* в данной работе будем называть элементы моноида $\widehat{A^*}$. В отличие от элементов моноида A^*, которые называются *конечными словами*, элементы из $\widehat{A^*} \setminus A^*$ будем называть *бесконечными псевдословами*. *Подсловом* данного слова на протяжении всей статьи будем называть

связную подпоследовательность букв данного слова. Мы также будем рассматривать подполугруппу $\widehat{A^+}$, которая получается из $\widehat{A^*}$ удалением нейтрального элемента (а именно пустого слова) и которая является свободной проконечной полугруппой над A.

Для более детального знакомства с теорией конечных и проконечных полугрупп мы отсылаем читателя к работам [2, 4, 5, 11, 17, 23].

Примером элементарного, но полезного наблюдения, немедленно вытекающего из компактности, служит следующая лемма.

Лемма 2.1. *Множество делителей элемента компактного моноида замкнуто.*

Мы будем свободно использовать тот факт, что замыкание $\overline{L}$ рационального языка $L \subseteq A^*$ в $\widehat{A^*}$ является открыто-замкнутым множеством, которое, кроме того, удовлетворяет равенству $\overline{L} \cap A^* = L$ (см. [2, § 3.6] или [5]). В частности, уместно заметить, что множество вида $\widehat{A^*}\,u\widehat{A^*}$ равно $\overline{A^*\,uA^*}$ и, следовательно, является открыто-замкнутым для любого $u \in A^*$. Другими словами, любой конечный набор элементов сходящейся последовательности конечных слов имеет данное конечное слово подсловом тогда и только тогда, когда предел этой последовательности включает в качестве подслова это слово. Аналогично, рассматривая языки вида $u\widehat{A^*} = \overline{uA^*}$, где $u \in A^+$, мы видим, что каждое бесконечное псевдослово имеет однозначно определённый конечный префикс (а двойственным образом и суффикс) любой конечной длины. На самом деле, если вычеркнуть этот префикс, остаток будет также однозначно определяться [2], но мы не будем использовать здесь этот результат. Кроме того, каждое открыто-замкнутое подмножество $\widehat{A^*}$ является замыканием некоторого рационального языка, так что топология нульмерного пространства $\widehat{A^*}$ точно отражает комбинаторику рациональных языков, но этого свойства мы также касаться не будем.

Для псевдослова $w \in \widehat{A^*}$ обозначим через $F(w)$ множество всех конечных подслов w и через $F_n(w)$ множество всех подслов w длины n.

Пусть w — бесконечное псевдослово. Говорят, что w *рекуррентно*, если для каждого $u \in F(w)$ найдётся такое слово v, что $uvu \in F(w)$. Назовём псевдослово w *равномерно рекуррентным*, если для каждого $u \in F(w)$ найдётся такое положительное целое N, что каждое $v \in F_N(w)$ имеет u своим подсловом. Заметим, что каждое равномерно рекуррентное псевдослово является рекуррентным. Рекуррентным будет и каждое слово минимального идеала I_A в $\widehat{A^*}$. С другой стороны, как видно из следующей леммы, если $|A| > 1$, то ни один элемент I_A не является равномерно рекуррентным.

Можно дать альтернативное определение рекуррентного псевдослова, позаимствовав его из символической динамики: будем называть бесконечное псевдослово рекуррентным, если все его бесконечные подслова имеют один и тот же набор конечных подслов. Такое определение оказывается эквивалентным равномерной рекуррентности, как показывает следующий результат.

Лемма 2.2. *Бесконечное псевдослово является равномерно рекуррентным тогда и только тогда, когда все его бесконечные подслова имеют один и тот же набор конечных подслов.*

Доказательство. Пусть w — бесконечное псевдослово. Предположим сначала, что оно равномерно рекуррентно. Пусть u — бесконечное подслово w. Тогда, разумеется, каждое конечное подслово u также является подсловом w. Обратно, так как слово u бесконечно, оно имеет конечные префиксы произвольной длины и поэтому имеет конечные подслова произвольной длины, которые также являются подсловами w. Поскольку w равномерно рекуррентное, каждое конечное подслово w будет подсловом любого достаточно длинного подслова и, следовательно, будет также подсловом слова u. Это означает, что u имеет один и тот же набор конечных подслов с псевдословом w.

Предположим далее, что все бесконечные подслова в w имеют один и тот же набор конечных подслов. Пусть v — некоторое конечное подслово псевдослова w. Рассуждая от противного, предположим, что найдётся произвольно длинное подслово w, не имеющее v своим подсловом. Тогда получим последовательность подслов в w, не имеющих подслова v, сходящуюся к некоторому бесконечному псевдослову u, которое само будет подсловом в w по лемме 2.1. Это означает, что u также не имеет подслова v, что противоречит предположению. Следовательно, w является равномерно рекуррентным. □

Цель этого раздела — получить характеризацию равномерной рекуррентности на алгебраическом языке. Для псевдослова w обозначим через $X(w)$ множество всех бесконечных псевдослов, являющихся пределами последовательностей конечных подслов в w, т. е. $X(w) = \overline{F(w)} \setminus A^*$.

Напомним, что о двух элементах s и t полугруппы S говорят, что s *лежит $\mathcal{J}$-выше* t, и пишут $s \geqslant_{\mathcal{J}} t$, если s — один из множителей (или *делителей*) в некотором разложении t на множители. Далее, говорят, что s и t *$\mathcal{J}$-эквивалентны*, если каждый из них является делителем другого. Будем писать $s >_{\mathcal{J}} t$, если $s \geqslant_{\mathcal{J}} t$, но s и t не $\mathcal{J}$-эквивалентны. Элемент s полугруппы S называется *регулярным*, если $sxs = s$ для некоторого $x \in S$. Хорошо известно, что для компактных полугрупп эквивалентны условия, что $\mathcal{J}$-класс целиком состоит из регулярных элементов, что хотя бы один элемент в этом $\mathcal{J}$-классе регулярен и что этот $\mathcal{J}$-класс содержит идемпотент. Отношение эквивалентности $\mathcal{J}$ — одно из отношений Грина на полугруппе S.

Заменяя слово «делитель» на «левый делитель» (или *префикс*), мы получим предпорядки $\geqslant_{\mathcal{R}}$ и $>_{\mathcal{R}}$ и отношение эквивалентности $\mathcal{R}$. Двойственным образом, заменяя «делитель» на «правый делитель» (или *суффикс*), мы получим предпорядки $\geqslant_{\mathcal{L}}$ и $>_{\mathcal{L}}$ и отношение эквивалентности $\mathcal{L}$. Пересечение отношений $\mathcal{R}$ и $\mathcal{L}$ обозначается $\mathcal{H}$. Вообще говоря, $\mathcal{J}$ не является наименьшим отношением, содержащим $\mathcal{R}$ и $\mathcal{L}$ (это отношение обозначается $\mathcal{D}$), но в каждой компактной полугруппе это так.

Каждая подгруппа полугруппы S (т. е. подполугруппа, являющаяся группой) содержится в некотором $\mathcal{J}$-классе, или, более точно, в некотором $\mathcal{H}$-классе. Те

$\mathcal{H}$-классы, которые являются подгруппами (а следовательно, максимальными подгруппами), — это в точности те $\mathcal{H}$-классы, которые содержат (единственный) идемпотент. Если полугруппа S компактна, то все максимальные подгруппы, содержащиеся в одном $\mathcal{J}$-классе, изоморфны как топологические группы. Компактные полугруппы удовлетворяют также следующему условию стабильности: если $x \leqslant_{\mathcal{R}} y$ и $x \mathcal{J} y$, то $x \mathcal{R} y$, и то же самое верно для отношения $\mathcal{L}$.

Лемма 2.3. *Пусть w — равномерно рекуррентное псевдослово над конечным алфавитом A.*

1. *Каждый элемент множества $X(w)$ является подсловом w.*
2. *Все элементы множества $X(w)$ находятся в одном $\mathcal{J}$-классе полугруппы $\widehat{A^*}$.*
3. *Каждый элемент множества $X(w)$ регулярен.*

Доказательство.

Утверждение 1 немедленно следует из леммы 2.1.

Докажем утверждение 2. Предположим, что $u, v \in X(w)$. Согласно лемме 2.2 u и v имеют одинаковые конечные подслова. Следовательно, по утверждению 1 u и v являются подсловами друг друга, т. е. они $\mathcal{J}$-эквивалентны.

Докажем утверждение 3. Пусть u — бесконечное псевдослово, являющееся пределом последовательности $(u_n)_n$ конечных подслов псевдослова w. Поскольку w рекуррентно и u_n — его конечные подслова, найдутся конечные подслова v_n, такие что $u_n v_n u_n$ тоже являются подсловами w. Если v — предельная точка последовательности $(v_n)_n$, то бесконечное псевдослово uvu принадлежит $X(w)$ и, следовательно, по утверждению 2 uvu $\mathcal{J}$-эквивалентно u. В компактных полугруппах это означает, что u — регулярный элемент. □

Для равномерно рекуррентного псевдослова w через $J(w)$ обозначим единственный $\mathcal{J}$-класс, содержащий множество $X(w)$.

Лемма 2.4. *Пусть w — равномерно рекуррентное псевдослово. Тогда в каждом $\mathcal{H}$-классе класса $J(w)$ содержится некоторый элемент множества $X(w)$.*

Доказательство. Пусть $u \in J(w)$. Обозначим x_n и y_n соответственно префикс и суффикс u длины n. Поскольку по лемме 2.2 u равномерно рекуррентно, в качестве y_n можно взять подслово u с ограниченным расстоянием слева и существует подслово t_n слова u длины по крайней мере $2n$, такое что x_n будет префиксом t_n, а y_n — суффиксом t_n. Пусть $(n_k)_k$ — строго возрастающая последовательность, такая что последовательности $(x_{n_k})_k$, $(y_{n_k})_k$ и $(t_{n_k})_k$ сходятся и x, y, t соответственно — их пределы. Согласно утверждению 2 леммы 2.3 $x, y, t \in J(w)$. Поскольку $x \geqslant_{\mathcal{R}} z \leqslant_{\mathcal{L}} y$ для $z \in \{u, t\}$, из стабильности следует, что u и t находятся в одном $\mathcal{H}$-классе. □

Лемма 2.5. *Пусть v — равномерно рекуррентное псевдослово. Предположим, что a — такая буква, что va тоже равномерно рекуррентное. Тогда v и va $\mathcal{R}$-эквивалентны.*

Доказательство. Пусть v_n — суффикс v длины n. Поскольку v является бесконечным подсловом равномерно рекуррентного псевдослова va, по лемме 2.2 они имеют одинаковые конечные подслова. Следовательно, для каждого n существует некоторое m_n, такое что имеет место разложение $v_{m_n} = x_n v_n a y_n$ для некоторых слов x_n, y_n. Из компактности следует, что существует некоторая строго возрастающая последовательность индексов $(n_k)_k$, такая что каждая из последовательностей $(v_{n_k})_k$, $(x_{n_k})_k$ и $(y_{n_k})_k$ сходится, скажем, к v', x и y соответственно. Тогда из непрерывности умножения в $\widehat{A^*}$ вытекает, что последовательность $(v_{m_{n_k}})_k$ сходится к $xv'ay$. Поскольку хорошо известно и легко проверить, что пределы двух сходящихся последовательностей суффиксов возрастающей длины и одного псевдослова $\mathcal{L}$-эквивалентны, получаем, что $v' \leqslant_{\mathcal{J}} v'a$ и, таким образом, $v' \mathcal{R} v'a$. Кроме того, так как v' — это предел последовательности суффиксов v, существует факторизация вида $v = zv'$. Поскольку $\mathcal{R}$-эквивалентность — левая конгруэнция, мы можем наконец заключить, что $va = zv'a \mathcal{R} zv' = v$. □

Теперь мы готовы сформулировать основной результат этого раздела.

Теорема 2.6. *Пусть w — бесконечное псевдослово над конечным алфавитом. Тогда w является равномерно рекуррентным в том и только в том случае, когда w $\mathcal{J}$-максимально как бесконечное псевдослово.*

Доказательство. Предположим сначала, что $w \in \widehat{A^*}$ является равномерно рекуррентным, и пусть $u \in J(w)$. По утверждению 1 леммы 2.3 $u \geqslant_{\mathcal{J}} w$, т. е. $w = puq$, где $p, q \in \widehat{A^*}$. Мы утверждаем, что $u \mathcal{J} w$. В самом деле, в противном случае согласно [2, следствие 5.6.2(b)] существует непрерывный гомоморфизм $\varphi\colon \widehat{A^*} \to M$ на конечный моноид, такой что $\varphi(u) >_{\mathcal{J}} \varphi(w)$. Покажем, что это приведёт к противоречию.

Пусть $(p_n)_n$ и $(q_n)_n$ — последовательности конечных слов, сходящиеся соответственно к p и q, такие что $\varphi(p_n) = \varphi(p)$ и $\varphi(q_n) = \varphi(q)$ для всех n. Рассматривая p_n и q_n для каждого n как произведение букв, мы можем видеть, что $\varphi(w)$ получается из $\varphi(u)$ с помощью последовательного умножения слева, а затем справа на образы относительно φ этих букв. Поскольку $\varphi(u) >_{\mathcal{J}} \varphi(w)$, на некотором шаге в этой последовательности умножений мы покинем $\mathcal{J}$-класс $\varphi(u)$. Другими словами, либо существует разложение вида $p_n = x_n a_n y_n$, где $a_n \in A$, такое что $\varphi(u) \mathcal{L} \varphi(y_n u) >_{\mathcal{L}} \varphi(a_n y_n u) \geqslant_{\mathcal{J}} \varphi(w)$, либо $\varphi(pu) = \varphi(p_n u) \mathcal{L} \varphi(u)$, причём в последнем случае существует разложение вида $q_n = z_n b_n t_n$, где $b_n \in A$, такое что $\varphi(pu) \mathcal{R} \varphi(puz_n) >_{\mathcal{R}} \varphi(puz_n b_n) \geqslant_{\mathcal{J}} \varphi(w)$. Поскольку алфавит конечен и $\widehat{A^*}$ — компакт, можно выделить такую подпоследовательность, что указанная последовательность букв постоянна, последовательность подслов сходится и это выполняется для каждого n. Следовательно, имеется либо некоторое разложение вида $p = xay$, где $a \in A$, такое что $\varphi(u) \mathcal{L} \varphi(yu) >_{\mathcal{L}} \varphi(ayu) \geqslant_{\mathcal{J}} \varphi(w)$, либо некоторое разложение вида $q = zbt$, где $b \in A$, такое что $\varphi(pu) \mathcal{R} \varphi(puz) >_{\mathcal{R}} \varphi(puzb) \geqslant_{\mathcal{J}} \varphi(w)$. Эти два случая, по существу, двойственны, так что мы рассмотрим только второй. Так как

$\varphi(puz) >_{\mathcal{R}} \varphi(puzb)$, нельзя сказать, что $puz\ \mathcal{R}\ puzb$. С другой стороны, как puz, так и $puzb$ — бесконечные подслова w, и поэтому по лемме 2.2 оба они равномерно рекуррентны. Значит, по лемме 2.5 имеем $puz\ \mathcal{R}\ puzb$. Полученное противоречие завершает доказательство утверждения.

Теперь для данного бесконечного подслова v псевдослова w обозначим через u бесконечный предел последовательности конечных префиксов подслова v. Тогда $u \in X(w) \subseteq J(w)$, и с помощью префиксной версии леммы 2.1 мы получим $u \geqslant_{\mathcal{R}} v \geqslant_{\mathcal{J}} w$. По условию $u\ \mathcal{J}\ w$, что означает, что $v\ \mathcal{J}\ w$. Следовательно, w $\mathcal{J}$-эквивалентно всем своим бесконечным подсловам, т. е. w является $\mathcal{J}$-максимальным как бесконечное псевдослово.

Обратно, предположим, что w $\mathcal{J}$-максимально как бесконечное псевдослово. Если v — бесконечное подслово в w, то вследствие $\mathcal{J}$-максимальности w имеем, что v $\mathcal{J}$-эквивалентно w. Поэтому v и w имеют одинаковые подслова и, в частности, одинаковые конечные подслова. По лемме 2.2 получаем, что w равномерно рекуррентно. □

Теорема 2.6 имеет несколько важных следствий, которые мы сейчас установим. Все доказательства представляют собой непосредственную проверку. Первое следствие могло быть также напрямую выведено из определения равномерно рекуррентного псевдослова.

Следствие 2.7. *$\mathcal{J}$-классы равномерно рекуррентных псевдослов целиком состоят из равномерно рекуррентных псевдослов.* □

Следствие 2.8. *$\mathcal{J}$-класс равномерно рекуррентного псевдослова w полностью определяется конечными подсловами w, а также конечными префиксами* (*соответственно суффиксами*) *псевдослова w.* □

Следствие 2.9. *Каждое равномерно рекуррентное псевдослово $\mathcal{H}$-эквивалентно пределу последовательности своих конечных подслов.* □

Следствие 2.10. *Если u и v — два равномерно рекуррентных псевдослова и каждое конечное подслово u является также подсловом v, то u и v $\mathcal{J}$-эквивалентны.* □

Назовём бесконечное псевдослово *периодическим*, если оно $\mathcal{J}$-эквивалентно некоторому псевдослову вида u^ω для некоторого $u \in A^+$. В завершение этого раздела приведём характеризацию свойства периодичности для равномерно рекуррентных псевдослов в терминах комбинаторных и топологических свойств множества их подслов. Основной идеей доказательства является лемма о накачке из теории автоматов, как и в доказательстве следствия 6.1.11 из [14].

Теорема 2.11. *Пусть $w \in \widehat{A^*}$ — равномерно рекуррентное псевдослово. Тогда эквивалентны следующие условия*:

1) *w периодическое*;
2) *язык $F(w)$ конечных подслов w рационален*;
3) *множество всех подслов w является открыто-замкнутым в $\widehat{A^*}$.*

Доказательство. Пусть F обозначает множество всех подслов w в $\widehat{A^*}$.

Докажем импликацию 1) $\Longrightarrow$ 3). Предположим, что w $\mathcal{J}$-эквивалентно u^ω, где $u \in A^+$. Тогда конечными подсловами w являются те слова, которые будут подсловами некоторой степени u. В частности, есть по меньшей мере n подслов w длины n. Согласно [10, теорема 6.3] подслова w являются подсловами u вместе со всеми словами вида $xu^\nu y$, где x — суффикс u, y — префикс u, a^ν обозначает произвольный элемент циклического свободного проконечного моноида $\widehat{\{a\}^*}$, а $u^\nu = \psi(a^\nu)$ для единственного непрерывного гомоморфизма $\psi\colon \widehat{\{a\}^*} \to \widehat{A^*}$, так что $\psi(a) = u$. Отсюда следует, что множество F является замыканием рационального языка

$$F(u) \cup \bigcup \{xu^*y\colon x \in (A^*)^{-1}u,\ y \in u(A^*)^{-1}\}$$

и поэтому является открыто-замкнутым множеством в $\widehat{A^*}$.

Проверим импликацию 3) $\Longrightarrow$ 2). Предположим, что множество F открыто и замкнуто. Тогда $F(w) = F \cap A^*$ — рациональный язык согласно [2, теорема 3.6.1].

Убедимся в справедливости импликации 2) $\Longrightarrow$ 1). Предположим, что $F(w)$ — рациональный язык. Тогда $F(w)$ распознается некоторым конечным детерминированным автоматом. Если этот автомат имеет n состояний и $v \in F \cap A^*$ — слово длины по крайней мере n, то v допускает разложение $v = xyz$, в котором $y \in A^+$ такое, что $xy^*z \subseteq F \cap A^*$. Это следует из леммы о накачке и того факта, что на пути, выходящем из начального состояния и помеченном словом v, некоторое состояние должно повториться. Из замкнутости F относительно образования подслов следует, что $y^* \subseteq F$. Так как F замкнуто, делаем вывод, что бесконечное псевдослово $y^\omega = \lim\limits_{n\to\infty} y^{n!}$ принадлежит F. Отсюда по теореме 2.6 мы заключаем, что $y^\omega\ \mathcal{J}\ w$, что обеспечивает периодичность w. □

3. Равномерная рекуррентность и подстановки

Итерация примитивных подстановок — это хорошо известный способ получения явления равномерной рекуррентности в символической динамике. Для псевдослов мы получили аналогичный результат, к представлению которого мы приступаем.

Для данного элемента x проконечного моноида последовательность $(x^{n!})_n$ должна сходиться к некоторому идемпотенту, причём имеется только один идемпотент, который является пределом последовательности положительных степеней x, просто потому что это так в каждом конечном моноиде, а проконечные моноиды финитно аппроксимируемы как топологические моноиды. Этот идемпотент, связанный с x, обозначается x^ω.

Мы уже показывали, что в случае, если проконечный моноид M конечно порождён, моноид непрерывных эндоморфизмов M является проконечным моноидом в топологии поточечной сходимости [5, теорема 4.14]. В частности, для

конечного алфавита A и для данного непрерывного эндоморфизма φ моноида $\widehat{A^*}$ имеется (единственный) идемпотент «бесконечная итерация» φ^ω.

Следующая лемма тривиальна, но существенна.

Лемма 3.1. *Если u — подслово $\varphi^\omega(v)$, то и $\varphi^\omega(u)$ — подслово $\varphi^\omega(v)$.*

Доказательство. По предположению u является подсловом в $\varphi^\omega(v)$, т. е. $\varphi^\omega(v) = xuy$, где $x, y \in \widehat{A^*}$. Так как φ^ω — идемпотентный гомоморфизм, то

$$\varphi^\omega(v) = \varphi^\omega(\varphi^\omega(v)) = \varphi^\omega(x)\varphi^\omega(u)\varphi^\omega(y),$$

что показывает, что $\varphi^\omega(u)$ является подсловом $\varphi^\omega(v)$. □

Так как $\widehat{A^*}$ является свободным проконечным моноидом на множестве A свободных порождающих, каждый гомоморфизм $\varphi\colon A^* \to B^*$ индуцирует непрерывный гомоморфизм $\hat{\varphi}\colon \widehat{A^*} \to \widehat{B^*}$. Говорят, что непрерывный гомоморфизм $\psi\colon \widehat{A^*} \to \widehat{B^*}$ является *конечным*, если ψ переводит конечное слово в конечное слово, т. е. ψ индуцирован некоторым гомоморфизмом $A^* \to B^*$. И гомоморфизм $A^* \to B^*$, и единственный индуцированный им конечный непрерывный гомоморфизм $\widehat{A^*} \to \widehat{B^*}$ называются *подстановками из A в B*, или просто *над A* в случае $B = A$.

Для псевдослова $w \in \widehat{A^*}$ через $c_{\leqslant n}(w)$ обозначается множество всех непустых подслов w длины не более n. Про элемент множества $c_{\leqslant n}(w)$ говорят также, что он *появляется в w*. Хорошо известно, что функция *содержания*, обозначаемая $c(w)$ и определяемая как $c(w) = c_{\leqslant 1}(w) \setminus \{1\}$, является непрерывным гомоморфизмом со значениями в полурешётке всех подмножеств A относительно объединения и дискретной топологии. Для $\varphi \in \operatorname{End}\widehat{A^*}$ положим $c_{\leqslant n}(\varphi) = \bigcup_{a\in A} c_{\leqslant n}(\varphi(a))$ и $c(\varphi) = c_{\leqslant 1}(\varphi) \setminus \{1\}$.

Лемма 3.2. *Пусть $\varphi \in \operatorname{End}\widehat{A^*}$. Тогда последовательность $\big(c(\varphi^n)\big)_n$ подмножеств A строго убывает до тех пор, пока не стабилизируется. В частности, $c(\varphi^\omega) = c(\varphi^{|A|})$.*

Доказательство. Если буква a появляется в $\varphi^{n+1}(b) = \varphi^n(\varphi(b))$, то имеется некоторая буква $d \in c(\varphi(b))$, такая что a появляется в подслове $\varphi^n(d)$. Следовательно, последовательность $(c(\varphi^n))_n$ не возрастает. Предположим далее, что $c(\varphi^n) = c(\varphi^{n+1})$. Для данной буквы $a \in c(\varphi^n)$ имеется некоторая буква b, такая что a появляется в $\varphi^{n+1}(b) = \varphi(\varphi^n(b))$. Следовательно, найдётся буква $d \in c(\varphi^n(b))$, такая что a появляется и в $\varphi(d)$. Поскольку $c(\varphi^n) = c(\varphi^{n+1})$, существует некоторая буква e, такая что $d \in c(\varphi^{n+1}(e))$. Тогда $a \in c(\varphi^{n+2})$, так как a появляется в $\varphi^{n+2}(e)$. □

Для $B \subseteq A$ обозначим $B^{\leqslant n}$ множество всех слов из букв B длины не более n. Мы скажем, что отображение $\varphi\colon \widehat{A^*} \to \widehat{B^*}$ *стирает* букву a, если $\varphi(a) = 1$.

Лемма 3.3. *Пусть $\varphi \in \operatorname{End}\widehat{A^*}$, и пусть $B = c(\varphi^\omega)$. Тогда если φ не стирает буквы из B, то последовательность $\big(c_{\leqslant r}(\varphi^n|_B)\big)_n$ подмножеств $B^{\leqslant n}$ строго возрастает до тех пор, пока не стабилизируется.*

Доказательство. Если u — подслово $\varphi^n(a)$ и $a \in B$, то $a \in c(\varphi(b))$ для некоторой буквы $b \in B$, и тогда u является подсловом $\varphi^{n+1}(b)$. Это означает, что последовательность возрастающая. Предположим далее, что $c_{\leqslant r}(\varphi^n|_B) = c_{\leqslant r}(\varphi^{n+1}|_B)$, и пусть u — подслово $\varphi^{n+2}(a)$ для некоторого $a \in B$. Поскольку $\varphi^{n+2}(a) = \varphi(\varphi^{n+1}(a))$, существует некоторое подслово v слова $\varphi^{n+1}(a)$, такое что u является подсловом $\varphi(v)$. Если мы возьмём в качестве v подслово минимальной длины (это возможно, так как φ не стирает буквы B), то мы должны получить $|v| \leqslant r$. Следовательно, v принадлежит $c_{\leqslant r}(\varphi^{n+1}|_B)$, а также и $c_{\leqslant r}(\varphi^n|_B)$. Это означает, что $u \in c_{\leqslant r}(\varphi^{n+1}|_B)$. Отсюда по индукции вытекает, что последовательность $\bigl(c_{\leqslant r}(\varphi^n|_B)\bigr)_n$ стабилизируется, как только повторится некоторый её член. □

Говорят, что непрерывный гомоморфизм φ моноида $\widehat{A^*}$ является *слабо примитивным*, если существует такое n, что множество $c_{\leqslant 2}(\varphi^n(a))$ одно и то же для каждой буквы $a \in A$ и не содержится в A, т. е. $\varphi^n(a)$ имеет по крайней мере одно подслово длины 2. Мы также скажем, что φ является *примитивным*, если существует такое n, что $c(\varphi^n(a)) = A$ для каждой буквы $a \in A$. Эндоморфизм моноида A^* называют *слабо примитивным* (соответственно *примитивным*), если его единственное продолжение до непрерывного эндоморфизма на $\widehat{A^*}$ обладает таким же свойством.

Лемма 3.4. *Пусть $\varphi \in \operatorname{End}\widehat{A^*}$. Предположим, что $c_{\leqslant 2}(\varphi^n(a))$ — одно и то же множество для всех $a \in A$ и фиксированного n. Тогда для каждого $m \geqslant n$ множество $c_{\leqslant 2}(\varphi^m(a))$ также не зависит от $a \in A$.*

Доказательство. Рассуждая по индукции, достаточно показать, что если $a, b \in A$ и u является подсловом $\varphi^{n+1}(a)$ длины не более 2, то u также является подсловом $\varphi^{n+1}(b)$. В самом деле, поскольку $\varphi^{n+1}(a) = \varphi(\varphi^n(a))$ и $|u| \leqslant 2$, существует такое $v \in c_{\leqslant 2}(\varphi^n(a))$, что u является подсловом $\varphi(v)$. Следовательно, $v \in c_{\leqslant 2}(\varphi^n(b))$, и u также является подсловом $\varphi^{n+1}(b)$. □

Для данного $c_{\leqslant 2}(w)$ множество элементов $w \in \widehat{A^*}$ — это пересечение конечного множества открыто-замкнутых подмножеств $\widehat{A^*}$, каждое из которых отвечает за присутствие или отсутствие некоторого подслова длины не больше 2. Поэтому функция $c_{\leqslant 2}\colon \widehat{A^*} \to \mathcal{P}(A^{\leqslant 2})$ является непрерывной в дискретной топологии множества всех подмножеств $\mathcal{P}(A^{\leqslant 2})$. Принимая во внимание лемму 3.4, мы заключаем, что $\varphi \in \operatorname{End}\widehat{A^*}$ является слабо примитивным тогда и только тогда, когда множество $c_{\leqslant 2}(\varphi^\omega(a))$ одно и то же для каждой буквы $a \in A$, и в этом случае оно совпадает с $c_{\leqslant 2}(\varphi^\omega)$. Поскольку $c(w) = c_{\leqslant 2}(w) \cap A$ для каждого $w \in \widehat{A^*}$, если φ является слабо примитивным, то мы также имеем $c(\varphi^\omega(a)) = c(\varphi^\omega)$ для каждой буквы $a \in A$.

Следующий результат полезен для выполнения вычислений в конкретных примерах. Он вытекает из сходного результата в теории Перрона—Фробениуса неотрицательных матриц, который был приведён (без доказательства) Виландтом [24], указавшим также пример, подтверждающий точность оценки. Доказательство имеется, например, в [20].

Лемма 3.5. *Пусть φ — слабо примитивная подстановка, $B = c(\varphi^\omega)$, $r = |B|$ и $N = r^2 - 2r + 2$. Тогда $c(\varphi^N(b)) = B$ для каждого $b \in B$.* □

Часть из следующих несложных наблюдений уже опубликована в [10], но ради полноты доказательства мы приводим их и здесь.

Лемма 3.6. *Пусть $\varphi \in \operatorname{End}\widehat{A^*}$.*

1. *Если $c(\varphi^\omega(a)) = B$ для каждой буквы $a \in A$, то все псевдослова $\varphi^\omega(a)$, где $a \in B$, лежат в одном и том же $\mathcal{J}$-классе.*
2. *Если все псевдослова $\varphi^\omega(a)$, где $a \in A$, лежат в одном $\mathcal{J}$-классе, то для каждого $n \geqslant 1$ множество $c_{\leqslant n}(\varphi^\omega(a))$ одно и то же для каждой буквы $a \in A$.*
3. *Если все $\varphi^\omega(a)$, где $a \in A$, имеют одни и те же подслова длины не более 2, то они имеют один и тот же набор конечных подслов.*

Доказательство.

1. Пусть $a, b \in B$. Предположим, что a является подсловом в $\varphi^\omega(b)$. Тогда по лемме 3.1 $\varphi^\omega(a)$ — подслово в $\varphi^\omega(b)$. В силу симметрии отсюда следует, что псевдослова $\varphi^\omega(a)$ и $\varphi^\omega(b)$ $\mathcal{J}$-эквивалентны.

2. Для данных $a, b \in A$ псевдослова $\varphi^\omega(a)$ и $\varphi^\omega(b)$ имеют одни и те же подслова, в частности одни и те же конечные подслова.

3. Достаточно показать, что для данных $a, b \in A$ каждое конечное подслово $\varphi^\omega(a)$ является также подсловом $\varphi^\omega(b)$. По [10, лемма 7.2] каждое конечное подслово u псевдослова $\varphi^\omega(a) = \varphi^\omega(\varphi^\omega(a))$ является также подсловом $\varphi^\omega(x)$ для некоторого подслова x псевдослова $\varphi^\omega(a)$ длины не больше 2. Тогда по предположению x является подсловом в $\varphi^\omega(b)$, и следовательно, по лемме 3.1 $\varphi^\omega(x)$ также является подсловом в $\varphi^\omega(b)$. Значит, u является подсловом в $\varphi^\omega(b)$. □

Из леммы 3.6 следует, что примитивные подстановки слабо примитивны. Примером слабо примитивной не примитивной подстановки может служить подстановка φ над алфавитом $\{a, b, c\}$, определённая так: $\varphi(a) = ab$, $\varphi(b) = ba$, $\varphi(c) = a^3b^3$. Здесь для каждой буквы x подслово в $\varphi^3(x)$ длины не больше 2 — это слово над алфавитом $\{a, b\}$.

Принимая во внимание лемму 3.6, для слабо примитивной подстановки $\varphi \in \operatorname{End}\widehat{A^*}$, где $B = c(\varphi^\omega)$, мы должны получить $c_{\leqslant n}(\varphi^\omega) = c_{\leqslant n}(\varphi^\omega|_B)$, что вместе с леммой 3.3 даёт простой алгоритм вычисления множеств $c_{\leqslant n}(\varphi^\omega)$. Грубую оценку сверху числа необходимых итераций даёт равенство $c_{\leqslant n}(\varphi^\omega) = c_{\leqslant n}((\varphi|_B)^M)$, где $M = \sum_{i=1}^{n} |B|^i = O(|B|^n)$, которое следует из леммы 3.3.

Теорема 3.7. *Пусть φ — подстановка над конечным алфавитом A. Тогда эквивалентны следующие условия*:

1) *все псевдослова $\varphi^\omega(a)$, где $a \in A$, $\mathcal{J}$-эквивалентны*;
2) *все псевдослова $\varphi^\omega(a)$, где $a \in A$, равномерно рекуррентны и имеют одинаковое содержание*;
3) *φ является слабо примитивным.*

Доказательство. Импликация 1) $\implies$ 3) следует из утверждения 2 леммы 3.6.

Чтобы доказать импликацию 2) $\implies$ 1), рассмотрим букву $b \in c(\varphi^\omega)$. По предположению b является подсловом в $\varphi^\omega(a)$ для каждого $a \in A$, и следовательно, $\varphi^\omega(b)$ также является подсловом в $\varphi^\omega(a)$ согласно лемме 3.1. Так как псевдослово $\varphi^\omega(b)$ само является равномерно рекуррентным, оно должно быть бесконечным. Из теоремы 2.6 мы выводим, что все псевдослова $\varphi^\omega(a)$ лежат в том же $\mathcal{J}$-классе, что и $\varphi^\omega(b)$, поскольку равномерно рекуррентное псевдослово не имеет бесконечных псевдослов, строго $\mathcal{J}$-выше его.

Чтобы закончить доказательство, осталось показать, что 3) $\implies$ 2), т. е. что слабая примитивность φ влечёт равномерную рекуррентность $\varphi^\omega(a)$, так как свойство совпадения содержаний в 2) немедленно следует из слабой примитивности. По утверждению 3 леммы 3.6 все псевдослова $\varphi^\omega(a)$, где $a \in A$, имеют одинаковые конечные подслова. Зафиксируем $a \in A$, и пусть v — конечное подслово $\varphi^\omega(a)$. Так как $\varphi^\omega(a) = \lim\limits_{n\to\infty} \varphi^{n!}(a)$ и все $\varphi^\omega(b)$ имеют одинаковые конечные подслова, для каждого $b \in A$ существует такое $k \geqslant 1$, что v — подслово в $\varphi^k(b)$. Поскольку b является подсловом в $\varphi^p(a)$ для всех $a \in A$ и всех достаточно больших p, существует такое k, что v будет подсловом в $\varphi^j(b)$ для всех $j \geqslant k$. Следуя [21, § 5.2], положим

$$K = \max_{b\in A} \min\{k \geqslant 1 \colon j \geqslant k \implies v \in F(\varphi^j(b))\}.$$

Пусть l — максимум длины $|\varphi^K(b)|$ для $b \in A$. Тогда подслово z псевдослова $\varphi^\omega(a)$ длины $2l-1$ должно быть $\varphi^r(a)$ для некоторого $r \geqslant K$. Заметим, что $\varphi^r(a)$ является произведением слов вида $\varphi^K(b)$ ($b \in A$), каждое из которых имеет слово v как подслово. Но z — слишком длинное подслово в $\varphi^r(a)$, чтобы покрыть эти слова, но не содержать целиком одно из них в качестве подслова. Значит, v является подсловом в z, что показывает, что псевдослово $\varphi^\omega(a)$ равномерно рекуррентно. □

Теперь мы исследуем, что случится, если применить конечный непрерывный эндоморфизм к равномерно рекуррентному псевдослову.

Теорема 3.8. *Пусть $\varphi\colon \widehat{A^*} \to \widehat{B^*}$ — конечный непрерывный гомоморфизм, и пусть псевдослово $w \in \widehat{A^*}$ таково, что φ не стирает ни одной буквы из $c(w)$. Тогда если w равномерно рекуррентно, то и псевдослово $\varphi(w)$ равномерно рекуррентно.*

Доказательство. Пусть w равномерно рекуррентно. Заметим, что $\varphi(w)$ является бесконечным псевдословом, так как φ не стирает никакую букву из w и никакая буква не может появиться конечное число раз в равномерно рекуррентном псевдослове.

Предположим, что v — конечное подслово $\varphi(w)$. Согласно следствию 2.9 существует последовательность $(w_n)_n$ конечных подслов w, сходящаяся к псевдослову в $\mathcal{H}$-классе псевдослова w. Так как φ — непрерывный гомоморфизм,

последовательность $(\varphi(w_n))_n$ подслов в $\varphi(w)$ сходится к некоторому псевдослову, $\mathcal{H}$-эквивалентному $\varphi(w)$ и, следовательно, имеющему те же конечные подслова, что и $\varphi(w)$. Значит, v является подсловом некоторого слова $\varphi(w_n)$. Пусть число N таково, что каждое подслово в w длины N содержит w_n как подслово. Пусть $K = (N+1)M + 1$, где $M = \max\{|\varphi(a)|\colon a \in A\}$, и пусть z — подслово в $\varphi(w)$ длины K. Тогда z является подсловом некоторого $\varphi(w_m)$, которое, в свою очередь, является произведением слов вида $\varphi(a)$. Теперь z можно выбрать достаточно длинным, чтобы оно содержало подслово вида $\varphi(y)$, где y — подслово в w_m длины N. Значит, w_n является подсловом y и, таким образом, v — подслово $\varphi(y)$, которое, в свою очередь, является подсловом z. Это показывает, что $\varphi(w)$ равномерно рекуррентно. □

Мы скажем, что подгруппа моноида $\widehat{A^*}$ является *$\mathcal{J}$-максимальной*, если она состоит из бесконечных псевдослов и никакая другая такая подгруппа $\widehat{A^*}$ не лежит строго $\mathcal{J}$-выше её. Из теоремы 2.6 следует, что $\mathcal{J}$-максимальные подгруппы — это подгруппы, состоящие из равномерно рекуррентных псевдослов. Согласно утверждению 3 леммы 2.3 $\mathcal{J}$-класс, состоящий из равномерно рекуррентных псевдослов, содержит $\mathcal{J}$-максимальную подгруппу, а фактически, все его подгруппы $\mathcal{J}$-максимальны.

Пример 3.9. Пусть $A = \{a_1, \dots, a_m\}$, и пусть $w_i = \varphi^\omega(a_i)$, где $\varphi(a_i) = a_1 \dots a_{i-1} a_i^2 a_{i+1} \dots a_m$ для $i = 1, \dots, m-1$ и $\varphi(a_m) = a_1 \dots a_m$. Как показано в [10], псевдослова w_i свободно порождают свободную проконечную подгруппу H моноида $\widehat{A^*}$. По теоремам 3.7 и 2.6 это $\mathcal{J}$-максимальная подгруппа. Из результатов, приводимых ниже в разделах 4 и 5, следует, что H — это $\mathcal{H}$-класс моноида $\widehat{A^*}$, а значит, максимальная подгруппа.

Скажем, что равенство $u_1 \dots u_m = v_1 \dots v_n$, где $u_i, v_j \in \widehat{A^*}$, *приводимо*, если существуют такие индексы r и s, что $2 < r + s \leqslant m + n$ и $u_r \dots u_m = v_s \dots v_n$.

Пусть φ — непрерывный гомоморфизм $\widehat{A^*} \to \widehat{B^*}$. Мы скажем, что гомоморфизм φ является *кодированием*, если он инъективен. Согласно [19, предложение 2.1], в случае, когда φ конечен, φ является кодированием тогда и только тогда, когда его ограничение на A^* инъективно.

Мы скажем, что множество $C \subseteq A^*$ — множество *с ограниченным запаздыванием по отношению к данному* $w \in \widehat{A^*}$, если существует такое целое число N, что любое равенство между подсловами w вида

$$uc_1 \dots c_m v = c'_1 \dots c'_n \quad \text{или} \quad uc_1 \dots c_m = c'_1 \dots c'_n v,$$

где $c_i, c'_j \in C$, $u, v \in A^*$ такие, что $A^*u \cap C^* \neq \varnothing$ и $vA^* \cap C^* \neq \varnothing$, и $m + n > N$, является приводимым. В этом случае говорят также, что C имеет *запаздывание не более N по отношению к w*. В случае, когда целое N таково, что C имеет запаздывание не более N по отношению к любому $w \in \widehat{A^*}$, мы также скажем, что C *имеет ограниченное запаздывание* и C *имеет запаздывание не более N*. Эффективные процедуры проверки этого сильного свойства в случае, если C конечно, описаны в [1, 22]. Из этих процедур нетрудно получить

алгоритм для проверки, имеет ли C ограниченное запаздывание по отношению к данному $w \in \widehat{A^*}$, в случае, если можно эффективно проверить, является ли некоторое конечное слово (зависящее только от C) подсловом w или нет.

Мы скажем, что конечный непрерывный гомоморфизм $\varphi\colon \widehat{A^*} \to \widehat{B^*}$ — гомоморфизм *с ограниченным запаздыванием по отношению к данному* $w \in \widehat{B^*}$, если $\varphi(A)$ является таковым. Мы также скажем, что φ имеет *запаздывание не более* N *по отношению к* w, если $\varphi(A)$ является таковым.

Следующий результат частично обращает теорему 3.8, которая будет играть ключевую роль в разделе 4.

Теорема 3.10. *Пусть* $\varphi\colon \widehat{A^*} \to \widehat{B^*}$ *— конечный непрерывный гомоморфизм, и пусть* $w \in \widehat{A^*}$. *Если псевдослово* $\varphi(w)$ *равномерно рекуррентно и* φ *является кодированием с ограниченным запаздыванием по отношению к* $\varphi(w)$, *то* w *также является равномерно рекуррентным.*

Доказательство. Пусть N — такое целое число, что φ имеет запаздывание не более N по отношению к $\varphi(w)$. Пусть $u \in F(w)$. Пусть $n = \lceil |u|/N \rceil + 2$, пусть m и M — соответственно минимум и максимум длин слов в $\varphi(A)$. Так как псевдослово $\varphi(w)$ является равномерно рекуррентным и A конечно, существует такое целое K, что любое конечное подслово $\varphi(w)$ длины не меньше K содержит в качестве подслова каждое подслово $\varphi(w)$ длины не больше MnN.

Пусть v — подслово в w длины $\lceil K/m \rceil$. Тогда $\varphi(v)$ является подсловом в $\varphi(w)$ длины не меньше K, которое, следовательно, содержит в качестве подслова некоторое слово вида $\varphi(xuy)$, где $x, y \in A^N$, так как длина такого слова не превосходит MnN. Пусть $v = v_1 \dots v_p$, $x = x_1 \dots x_N$, $u = u_1 \dots u_q$ и $y = y_1 \dots y_N$, где $v_i, x_j, u_k, y_j \in A$. Обозначим для каждого $a \in A$ $\varphi(a)$ через $\bar{a}$. Тогда мы имеем равенство между подсловами $\varphi(w)$ вида

$$\bar{v}_1 \dots \bar{v}_p = z\,\bar{x}_1 \dots \bar{x}_N\,\bar{u}_1 \dots \bar{u}_q\,\bar{y}_1 \dots \bar{y}_N\,t$$

для некоторых $z, t \in A^*$. Так как φ имеет запаздывание не более N по отношению к $\varphi(w)$, существуют индексы i, j, k, l, такие что

$$\bar{v}_i \dots \bar{v}_j = \bar{x}_k \dots \bar{x}_N \bar{u}_1 \dots \bar{u}_q \bar{y}_1 \dots \bar{y}_l.$$

Поскольку φ является кодированием, последнее равенство останется верным, если удалить верхние чёрточки, и значит, u является подсловом v. Поэтому w равномерно рекуррентно. □

Заметим, что для произвольного нестирающего непрерывного гомоморфизма $\varphi\colon \widehat{A^*} \to \widehat{B^*}$ уже нельзя ожидать, что w будет равномерно рекуррентным только потому, что $\varphi(w)$ является равномерно рекуррентным. Действительно, просто заменив одно вхождение некоторой буквы в равномерно рекуррентном псевдослове v на новую букву, мы получим псевдослово w, уже не являющееся равномерно рекуррентным. Однако, полагая φ тождественным на всех старых буквах и переводящим новую букву в заменённую ей букву, мы будем иметь $\varphi(w) = v$. В этом примере φ не является кодированием. Мы не знаем, имеются

ли примеры, в которых φ является кодированием, не удовлетворяющим предположению об ограниченности запаздывания из теоремы 3.10, и не сохраняет равномерную рекуррентность.

4. Слабо примитивные подстановки

На протяжении этого раздела φ будет обозначать конечный слабо примитивный непрерывный эндоморфизм $\widehat{A^*}$, где A — конечный алфавит. Согласно теореме 3.7 все псевдослова $\varphi^\omega(a)$ ($a \in A$) лежат в одном $\mathcal{J}$-классе $\widehat{A^*}$. Мы обозначим этот $\mathcal{J}$-класс через J_φ. Подслова элементов из J_φ будем называть просто *подсловами из* J_φ. По теореме 2.6 и утверждению 3 леммы 2.3 J_φ является $\mathcal{J}$-максимальным регулярным $\mathcal{J}$-классом $\widehat{A^+}$ и состоит из равномерно рекуррентных псевдослов. Поэтому бесконечные подслова из J_φ являются членами J_φ. Из компактности и непрерывности умножения вытекает, что множество подслов из J_φ замкнуто.

Лемма 4.1.

1. *Если u — бесконечное подслово из J_φ, то таковым является и $\varphi(u)$.*
2. *Если u — непустое подслово из J_φ, то $\varphi^\omega(u) \in J_\varphi$.*

Доказательство.

1. Пусть a — любая буква в $c(\varphi^\omega)$, и пусть $w = \varphi^\omega(a)$. Так как $w = \lim\limits_{n\to\infty} \varphi^{n!}(a)$, u является конечным подсловом w и множество $\widehat{A^*}u\widehat{A^*}$ открыто в $\widehat{A^*}$, u должно быть подсловом $\varphi^{n!}(a)$ для всех достаточно больших n. Так как φ слабо примитивен, для всех достаточно больших m буква a появляется в $\varphi^{m-n!}(a)$ и, таким образом, слово $\varphi^{n!}(a)$ является подсловом $\varphi^m(a)$. Значит, для всех достаточно больших m псевдослово u является подсловом в $\varphi^m(a)$ и, следовательно, подсловом в $\varphi^{\omega-1}(a) = \lim\limits_{n\to\infty} \varphi^{n!-1}(a)$. Поскольку φ — гомоморфизм, $\varphi(u)$ является подсловом в $\varphi^\omega(a) = w$.

2. По лемме 3.1 $\varphi^\omega(u)$ — бесконечное подслово из J_φ. Значит, $\varphi^\omega(u) \in J_\varphi$, так как J_φ является $\mathcal{J}$-максимальным $\mathcal{J}$-классом бесконечных псевдослов. □

Предложение 4.2. *Действие φ на $\widehat{A^*}$ индуцирует действие на J_φ.*

Доказательство. Возьмём $a \in A$ и положим $w = \varphi^\omega(a)$. Так как псевдослово w равномерно рекуррентно по теореме 3.7, по теореме 3.8 псевдослово $\varphi(w)$ также равномерно рекуррентно. Значит, согласно следствию 2.10 достаточно показать, что каждое конечное подслово в $\varphi(w)$ является также подсловом в w. Теперь по [10, лемма 7.2] каждое конечное подслово u из $\varphi(w)$ является подсловом в $\varphi(v)$ для некоторого конечного подслова v псевдослова w. Кроме того, по утверждению 1 леммы 4.1 как только v будет конечным подсловом w, таким будет и $\varphi(v)$. Значит, u является подсловом в w. □

Лемма 4.3. *Пусть v — псевдослово из J_φ, принадлежащее $\operatorname{Im}\varphi^\omega$, и пусть a — его первая буква. Тогда a будет также первой буквой в $\varphi^\omega(a)$ и найдётся некоторое $k \geqslant 1$, такое что a — первая буква в $\varphi^k(a)$ и $\varphi^{\omega-k}(a) \in J_\varphi$.*

Доказательство. По предположению имеется разложение вида $v = av'$ для некоторого $v' \in \widehat{A^+}$. Таким образом, первая буква a из $v = \varphi^\omega(v) = \varphi^\omega(a)\varphi^\omega(v')$ является также первой буквой в $\varphi^\omega(a)$. Поскольку алфавит A конечен, множество $a\widehat{A^*}$ открыто и найдётся некоторое $k \geqslant 1$, такое что $\varphi^k(a)$ начинается с буквы a. Из утверждения 4.2 и замкнутости J_φ имеем

$$\varphi^{\omega-k}(a) = \varphi^{\omega-k}(\varphi^\omega(a)) = \lim_{n\to\infty} \varphi^{n!-k}(\varphi^\omega(a)),$$

т. е. $\varphi^{\omega-k}(a)$ также лежит в J_φ. □

Лемма 4.4. *Пусть H — максимальная подгруппа в J_φ, содержащая элемент вида $\varphi^\omega(v)$ для некоторого псевдослова v. Тогда $\varphi^\omega(H) \subseteq H$.*

Доказательство. Пусть $K = \varphi^\omega(H)$. Тогда K — непрерывный гомоморфный образ проконечной группы. Поскольку K — замкнутая подполугруппа проконечной полугруппы, она сама является проконечной полугруппой [4, предложение 4.3]. Значит, K — проконечная группа согласно тому же результату. С другой стороны, $H \cap K$ не пусто, так как оба множества содержат псевдослово $\varphi^\omega(v)$. Из того, что H — максимальная подгруппа в $\widehat{A^*}$, следует, что $K \subseteq H$. □

Пусть a и b — такие буквы, что ba является подсловом из J_φ. Обозначим через $X_\varphi(a,b)$ множество всех таких конечных слов u, что bua — подслово из J_φ и u начинается с a, заканчивается на b и не может быть собственным образом разложено в произведение таких слов, т. е. не содержит подслова ba. Есть другое, более широкое, вообще говоря, множество, связанное с $X_\varphi(a,b)$, которое также играет некоторую роль. Это множество $Y_\varphi(a,b)$, состоящее из всех конечных подслов из J_φ, которые начинаются с a, заканчиваются на b и не содержат подслов ba. Так как элементы J_φ равномерно рекуррентны, множество $Y_\varphi(a,b)$ конечно, и поэтому конечно и его подмножество $X_\varphi(a,b)$. Более точно, мы имеем следующий результат, который показывает, что $X_\varphi(a,b)$ может быть эффективно вычислено.

Лемма 4.5. *Пусть ba — двубуквенное подслово из J_φ, $B = c(\varphi^\omega)$ и $r = |B|$. Пусть M — наименьшее целое, такое что $c_{\leqslant 2}(\varphi^M) = c_{\leqslant 2}(\varphi^{M+1})$, а N — наименьшее целое, такое что $c(\varphi^N(b)) = c(\varphi^\omega)$ для каждого $b \in B$. Тогда $X_\varphi(a,b)$ состоит из подслов слов вида $\varphi^{M+N}(u)$, где $u \in c_{\leqslant 2}(\varphi^\omega|_B)$. Поэтому $X_\varphi(a,b)$ может быть эффективно вычислено.*

Доказательство. Пусть $w \in X_\varphi(a,b)$. Тогда w является подсловом из J_φ и, следовательно, подсловом $\varphi^{M+N}(u)$ для некоторого $u \in B^*$. По лемме 3.3 ba — подслово $\varphi^M(d)$ для некоторого $d \in B$. С другой стороны, по предположению d появляется в каждом слове вида $\varphi^N(e)$, где $e \in B$. Значит, ba является подсловом каждого слова вида $\varphi^{M+N}(e)$, где $e \in B$. Поскольку w не содержит подслова

ba, w не может содержать и любого подслова вида $\varphi^{M+N}(e)$, где $e \in B$, и значит, оно должно быть подсловом $\varphi^{M+N}(u_0)$ для некоторого $u_0 \in c_{\leqslant 2}(\varphi^\omega|_B)$, что доказывает утверждение леммы. □

Отметим, что числа M и N из леммы 4.5 удовлетворяют следующим неравенствам: из леммы 3.3 следует, что $M \leqslant r^2$, и из леммы 3.5, что $N \leqslant r^2 - 2r + 2$. Верхняя граница для N оптимальна по [24], но верхняя оценка для M, вероятно, не является оптимальной.

Пример 4.6. Для подстановки $\varphi \in \operatorname{End} \widehat{\{a,b\}^*}$, которая переводит букву a в ab^2, а b в a, где $r = 2$, мы находим, что $N = 2$, $M = 3$ и каждое двубуквенное слово является подсловом из J_φ. Значит, чтобы вычислить множество $X_\varphi(a,a)$, достаточно вычислить слова

$$\varphi^5(a) = abbaaabbabbabbaaabbaaabbaaabbabbabbaaabbabb,$$
$$\varphi^5(b) = abbaaabbabbabbaaabbaa,$$

приписать их друг к другу в любом порядке и найти подслова между последовательными вхождениями подслова aa. Проделав это рутинное вычисление, мы заключаем, что $X_\varphi(a,a) = \{a, ab^2a, (ab^2)^3a\}$. Так как каждое слово из $Y_\varphi(a,a)$ является подсловом некоторого слова из $X_\varphi(a,a)$, немедленно получаем, что $Y_\varphi(a,a) = \{a, ab^2a, (ab^2)^2a, (ab^2)^3a\}$.

Для подмножества X полугруппы $\widehat{A^+}$ обозначим X^+ подполугруппу $\widehat{A^+}$, порождённую X.

Лемма 4.7. *Предположим, что ba является подсловом из J_φ и что имеется некоторое псевдослово вида $w = \varphi^\omega(u)$, где $u \in X_\varphi(a,b)$ такое, что w начинается с a и заканчивается на b. Пусть M — максимальная длина элемента из $X_\varphi(a,b)$, и пусть v — такое конечное слово, которое имеет тот же префикс длины $M+1$, тот же суффикс длины $M+1$ и то же подслово длины $M+2$, что и w. Тогда v принадлежит $X_\varphi(a,b)^+$.*

Доказательство. Заметим, что по выбору M каждое подслово длины $M+1$ равномерно рекуррентного псевдослова w должно содержать ba как подслово. Поскольку каждое подслово в w длины $M+1$ является подсловом в v, слово v должно содержать ba как подслово. Из того, что v начинается с a и заканчивается на b, следует, что v допускает разложение вида $u_1u_2\dots u_r$, где каждый множитель u_i начинается с a, заканчивается на b, не имеет ba подсловом и его длина не более M. Значит, u_1a — префикс, bu_r — суффикс, а каждое слово bu_ia $(1 < i < r)$ является подсловом в w. Кроме того, раз ba является подсловом из J_φ, то и $\varphi^\omega(ba)$ тоже является подсловом из J_φ. Из того, что псевдослово $\varphi^\omega(u)$ начинается с a и заканчивается на b, следует, что $\varphi^\omega(bua)$ принадлежит J_φ. Значит, bu_1a и bu_ra также являются подсловами в w по лемме 4.3. По определению множества $X_\varphi(a,b)$ это означает, что все подслова u_j принадлежат $X_\varphi(a,b)$. Значит, $v \in X_\varphi(a,b)^+$. □

Предложение 4.8. *Пусть a и b — такие буквы, что ba является подсловом из J_φ.*

1. *Все псевдослова вида $\varphi^\omega(u)$, где $u \in X_\varphi(a,b)$, принадлежат одному $\mathcal{H}$-классу H в J_φ, который является группой.*
2. *Если $\varphi^\omega(a)$ начинается с a, а $\varphi^\omega(b)$ заканчивается на b, то $\varphi^\omega(H)$ порождается множеством $\varphi^\omega(X_\varphi(a,b))$ как замкнутая подгруппа.*

Доказательство. Псевдослова $\varphi^\omega(a)$ и $\varphi^\omega(b)$, как, согласно утверждению 2 леммы 4.1, и все элементы множества $\varphi^\omega(X_\varphi(a,b))$, принадлежат J_φ. Кроме того, $\varphi^\omega(a)$ является префиксом, а $\varphi^\omega(b)$ — суффиксом каждого элемента из $\varphi^\omega(X_\varphi(a,b))$. Значит, $\varphi^\omega(X_\varphi(a,b))$ содержится в $\mathcal{H}$-классе H, который является пересечением $\mathcal{R}$-класса $\varphi^\omega(a)$ и $\mathcal{L}$-класса $\varphi^\omega(b)$.

Так как ba является подсловом из J_φ, а псевдослова из J_φ равномерно рекуррентны, имеется некоторое конечное подслово из J_φ вида $baubavba$, которое также имеет вид xy, где $x, y \in X_\varphi(a,b)$. Снова по утверждению 2 леммы 4.1 псевдослово $\varphi^\omega(xy) = \varphi^\omega(x)\varphi^\omega(y)$ принадлежит J_φ, что означает, что H — группа. Это доказывает утверждение 1. Кроме того, по лемме 4.4 $\varphi^\omega(H)$ является проконечной подгруппой на H.

Предположим, далее, что $\varphi^\omega(a)$ начинается на a, а $\varphi^\omega(b)$ заканчивается на b. Тогда каждый элемент из H начинается на a и заканчивается на b.

Пусть M выбрано как в лемме 4.7, и пусть w — произвольный элемент $\varphi^\omega(H)$. Пусть $(w_n)_n$ — последовательность конечных слов, сходящаяся к w, которую мы можем выбрать так, чтобы все w_n имели такой же префикс и такой же суффикс длины $M+1$, как и w, а также такие же подслова длины $M+2$, как у w. Из леммы 4.7 следует, что каждое w_n принадлежит $X_\varphi(a,b)^+$. Это показывает, что $w \in \overline{X_\varphi(a,b)^+}$. Из непрерывности φ^ω мы заключаем, что $\varphi^\omega(w)$ принадлежит замыканию $\varphi^\omega(X_\varphi(a,b))^+$. Наконец, из утверждения 1 следует, что замыкание подполугруппы $\varphi^\omega(X_\varphi(a,b))^+$ является замкнутой подгруппой в H, порождённой $\varphi^\omega(X_\varphi(a,b))$, что доказывает утверждение 2. □

Скажем, что φ — конечная слабо примитивная подстановка на алфавите A *с взаимно ограниченным запаздыванием*, если φ имеет ограниченное запаздывание по отношению к элементам из J_φ, и скажем, что подстановка φ является *специальной*, если φ — подстановка с взаимно ограниченным запаздыванием и ограничение φ на $\widehat{c(\varphi^\omega)^*}$ является кодированием.

Лемма 4.9. *Если φ — конечный специальный слабо примитивный непрерывный эндоморфизм моноида $\widehat{A^*}$, то и φ^n — конечный специальный слабо примитивный непрерывный эндоморфизм для любого $n \geqslant 1$.*

Доказательство. Пусть $B = c(\varphi^\omega)$. Так как φ по предположению — инъективный и непрерывный эндоморфизм $\widehat{B^*}$, его степени φ^n также будут обладать этими свойствами. Поскольку $\varphi^\omega = (\varphi^n)^\omega$ и, таким образом, $J_\varphi = J_{\varphi^n}$, осталось показать, что φ^n будет с ограниченным запаздыванием по отношению к элементам из J_φ. Для того чтобы доказать это для $n > 1$, предположим индуктивно, что φ^{n-1} будет с ограниченным запаздыванием по отношению к элементам из J_φ.

Рассмотрим равенство между подсловами в J_φ следующего вида:

$$u\varphi^n(a_1)\dots\varphi^n(a_r)v = \varphi^n(b_1)\dots\varphi^n(b_s), \tag{4.1}$$

где $a_i, b_j \in B$. Поскольку предполагается, что φ^{n-1} — гомоморфизм с ограниченным запаздыванием по отношению к подсловам из J_φ, в случае, если сумма $r+s$ достаточно велика, найдутся индексы i_1, j_1 и разложения $\varphi(a_{i_1}) = x_{i_1}x'_{i_1}$ и $\varphi(b_{j_1}) = y_{j_1}y'_{j_1}$, такие что

$$u\varphi^{n-1}(\varphi(a_1\dots a_{i_1-1})x_{i_1}) = \varphi^{n-1}(\varphi(b_1\dots b_{j_1-1})y_{j_1}), \tag{4.2}$$

$$\varphi^{n-1}(x'_{i_1}\varphi(a_{i_1+1}\dots a_r))v = \varphi^{n-1}(y'_{j_1}\varphi(b_{j_1+1}\dots b_s)). \tag{4.3}$$

Если $r+s$ достаточно велика, одно из чисел i_1+j_1, $r+s-i_1-j_1$ должно быть также достаточно большим, чтобы гарантировать, что по крайней мере одно из равенств (4.2), (4.3) будет приводиться подобным образом, доставляя, скажем, равенства

$$\begin{aligned} u\varphi^{n-1}(\varphi(a_1\dots a_{i_2-1})x_{i_2}) &= \varphi^{n-1}(\varphi(b_1\dots b_{j_2-1})y_{j_2}),\\ \varphi^{n-1}(x'_{i_2}\varphi(a_{i_2+1}\dots a_{i_1-1})x_{i_1}) &= \varphi^{n-1}(y'_{j_2}\varphi(b_{j_2+1}\dots b_{j_1-1})y_{j_1}), \end{aligned} \tag{4.4}$$

где $\varphi(a_{i_2}) = x_{i_2}x'_{i_2}$ и $\varphi(b_{j_2}) = y_{j_2}y'_{j_2}$. Снова предполагая, что сумма $r+s$ достаточно велика, мы можем выполнять преобразования такого же типа до тех пор, пока, приписывая равенства вида (4.4), не получим равенство вида

$$\varphi^{n-1}(x'_l\varphi(a_{l+1}\dots a_{m-1})x_m) = \varphi^{n-1}(y'_p\varphi(b_{p+1}\dots b_{q-1})y_q),$$

где $\varphi(a_t) = x_tx'_t$, $\varphi(b_t) = y_ty'_t$ и $m-l+q-p$ сколь угодно велико. Из того, что φ^{n-1} инъективен на B^*, $B = c(\varphi^\omega)$ и φ слабо примитивен, следует, что

$$x'_l\varphi(a_{l+1})\dots\varphi(a_{m-1})x_m = y'_p\varphi(b_{p+1})\dots\varphi(b_{q-1})y_q. \tag{4.5}$$

Кроме того, поскольку φ^{n-1} переводит J_φ в себя по предложению 4.2 и φ^{n-1} инъективен на $\widehat{B^*}$, общее значение обеих частей равенства (4.5) является подсловом из J_φ. Теперь, так как $m-l+q-p$ может быть взято сколь угодно большим и φ будет с ограниченным запаздыванием по отношению к подсловам из J_φ, мы заключаем, что равенство (4.5) приводимо, скажем, так:

$$x'_l\varphi(a_{l+1}\dots a_f) = y'_p\varphi(b_{p+1}\dots b_g).$$

Используя вычисления для получения равенства (4.5), имеем

$$u\varphi^n(a_1\dots a_f) = \varphi^n(b_1\dots b_g),$$

что показывает, что равенство (4.1) приводимо. Равенства другого типа, необходимые, чтобы показать, что φ^n будет с ограниченным запаздыванием по отношению к элементам из J_φ, рассматриваются сходным образом. □

Итак, при подходящих предположениях мы описали в утверждении 2 предложения 4.8 множества порождающих для замкнутой подгруппы $\varphi^\omega(H)$, соответствующей максимальной подгруппе H в J_φ. Сейчас нам понадобится дополнительное предположение об ограниченном запаздывании по отношению к элементам из J_φ, чтобы показать, что если H и $\varphi^\omega(H)$ имеют некоторую общую точку,

то они эквивалентны. Доказательство этого результата оказывается довольно длинным и техническим.

Предложение 4.10. *Пусть φ — специальный конечный слабо примитивный непрерывный эндоморфизм $\widehat{A^*}$, и пусть $w \in J_\varphi$. Если w лежит в том же $\mathcal{H}$-классе, что и некоторый элемент из $\operatorname{Im}\varphi^\omega$, то $w \in \operatorname{Im}\varphi^\omega$.*

Доказательство. Пусть v — тот элемент $\mathcal{H}$-класса w, который лежит в $\operatorname{Im}\varphi^\omega$. Так как φ^ω — идемпотентный гомоморфизм, мы имеем $\varphi^\omega(v) = v$. Заметим, что v и w имеют одинаковые подслова, а также одинаковые конечные префиксы и суффиксы. Так как $v = \lim\limits_{n\to\infty} v_n$ для некоторой последовательности $(v_n)_n$ конечных слов и потому $v = \varphi^\omega(v) = \lim\limits_{n\to\infty} \varphi^\omega(v_n)$, каждое конечное подслово в w является подсловом некоторого слова в $\varphi^k(A^+)$ для каждого положительного целого k.

Пусть a — первая буква v. По лемме 4.3 найдётся некоторое $l > 0$, такое что $\varphi^l(a)$ начинается с a. Далее, $(\varphi^l)^\omega = \varphi^\omega$ (и значит, $J_{\varphi^l} = J_\varphi$), так что, используя вычисления леммы 4.9 и заменяя φ на φ^l, если это необходимо, мы можем получить, что a — первая буква в $\varphi(a)$. Это означает, что $\varphi^n(a)$ является префиксом $\varphi^{n+1}(a)$ для всех $n \geqslant 0$, откуда $\varphi^n(a)$ является префиксом v для всех $n \geqslant 0$. В частности, w имеет произвольно длинные префиксы вида $\varphi^k(u)$, где $u \in A^+$ и $k > 0$. Аналогично, w имеет произвольно длинные суффиксы в $\varphi^k(A^+)$ для каждого $k > 0$.

Пусть k — произвольное положительное целое, и пусть $\psi = \varphi^k$. По лемме 4.9 существует такое N, что ψ имеет запаздывание не более N по отношению к w. Пусть m и M — соответственно минимальная и максимальная длины слов из $\psi(A)$, и пусть $K = \big(N + \lceil \frac{M}{m} \rceil + 2\big)M$.

Предположим, далее, что x — конечное слово, которое имеет одинаковые подслова, одинаковые префиксы и одинаковые суффиксы длины не более K с псевдословом w. Мы утверждаем, что $x \in \operatorname{Im}\psi$. Так как w имеет произвольно длинные префиксы в $\psi(A^+)$, x имеет префикс y_0 и суффикс z в $\psi(A^{N+\lceil \frac{M}{m} \rceil + 2})$.

С другой стороны, уже было отмечено, что произвольное подслово u длины K псевдослова w является подсловом некоторого слова из $\psi(A^+)$. Значит, u должно иметь вид $u = u_1u_2u_3u_4u_5u_6u_7$, где длина каждого из слов u_1 и u_7 меньше M, $|u_1u_2| = |u_6u_7| = M$, $u_2u_3, u_5u_6 \in \psi(A^+)$ и $u_4 = \psi(\tilde{u}_4)$ для некоторого $\tilde{u}_4 \in A^+$ длины не менее $N-2$. Заметим, что некоторые из множителей u_i, в частности u_3 и u_5, могут быть пустыми. Это разложение изображено на рис. 1, где подразумевается, что дуги представляют элементы из $\psi(A)$.

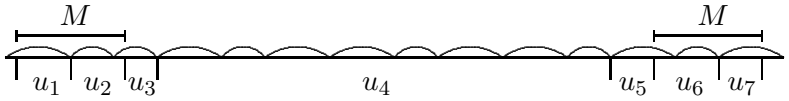


Рис. 1. Разложение множителя длины K

Далее, предположим, что мы уже идентифицировали префикс y_n слова x, который принадлежит $\psi(A^+)$, и что $K \leqslant |y_n| < |x| - M$. Пусть u — суффикс длины K префикса слова x длины $|y_n| + M$. Рассмотрим для него разложение $u = u_1u_2u_3u_4u_5u_6u_7$, описанное в предыдущем абзаце. Тогда префикс $u_2u_3u_4u_5$ слова $u_2u_3u_4u_5u_6$, являющегося произведением не менее N множителей из $\psi(A)$, будет также суффиксом слова y_n. Из того, что ψ имеет запаздывание не больше N по отношению к w, следует, что равенство, выражающее перекрытие множителей, должно расщепляться, так как оно предполагает два разложения на подслова слова u, а следовательно, и на подслова слова w. Значит, мы можем дальше расширить y_n, «перескакивая» от разложения внутри y_n к разложению слова u, и, следовательно, найти такое слово y_{n+1}, что $|y_{n+1}| > |y_n|$ и $y_{n+1} \in \psi(A^+)$. Расширение разложения префикса слова x в терминах элементов $\psi(A)$ изображено на рис. 2.

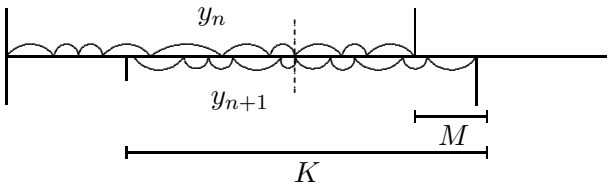


Рис. 2. Расширение разложения префикса слова x в $\psi(A^+)$

Предположим, что y — самый длинный префикс слова x, который принадлежит $\psi(A^+)$. Согласно предыдущему рассуждению и предположениям относительно x мы имеем $|y| \geqslant K$ и $|y| > |x| - M$. Мы утверждаем, что $y = x$. В противном случае рассмотрим перекрытие y с суффиксом z слова x, введённое выше. По соображениям длин имеем разложения $y = y't$ и $z = tz'$, где $1 \leqslant |z'| < M$ (см. рис. 3). Напомним, что z — это произведение $N + \lceil \frac{M}{m} \rceil + 2$ подслов из $\psi(A)$.

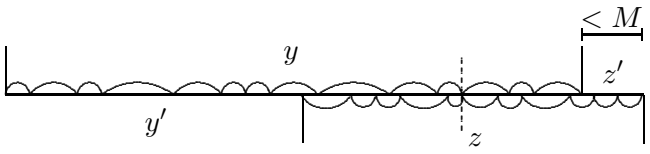


Рис. 3. Окончательное расширение префикса x в $\psi(A^+)$

Читая справа налево, исключим те подслова, которые лежат целиком внутри z', при этом, конечно, останется по крайней мере N подслов. Так как ψ имеет запаздывание не больше N по отношению к w, мы найдём разложение (на подслова слова w), включающее те оставшиеся подслова, которые должны расщепляться, что позволит нам расширить y до самого длинного префикса, всё ещё лежащего в $\psi(A^+)$. Это противоречит предположению, сделанному в начале абзаца, и завершает доказательство утверждения о том, что $x \in \psi(A^+)$.

Теперь, так как выписанное конечное число условий на конечные подслова определяет открыто-замкнутое подмножество моноида $\widehat{A^+}$, w является пределом последовательности $(z_n)_n$ конечных слов, имеющих те же подслова, те же префиксы и те же суффиксы длины K, что и w. Согласно рассуждениям выше, каждое z_n принадлежит $\psi(A^+)$. Из того, что $\psi = \varphi^k$ непрерывный, следует, что $w \in \operatorname{Im}\varphi^k$, скажем $w = \varphi^k(w_k)$.

Поскольку $\widehat{A^*}$ — компактное метрическое пространство, имеется строго возрастающая последовательность $(k_r)_r$, такая что $(w_{k_r!})_r$ сходится к некоторому псевдослову w_∞. Из непрерывности оценивающего отображения непрерывных эндоморфизмов моноида $\widehat{A^*}$ [5, теорема 4.14] мы выводим, что

$$w = \lim_{r\to\infty} \varphi^{k_r!}(w_{k_r!}) = \varphi^\omega(w_\infty),$$

поэтому $w \in \operatorname{Im}\varphi^\omega$. □

Для подмножества X группы G обозначим через $\langle X\rangle$ подгруппу, порождённую X.

Двубуквенное подслово ba из J_φ, такое что $\varphi^\omega(a)$ начинается с a, а $\varphi^\omega(b)$ заканчивается на b, будем называть *связью* для φ. Это название указывает на то, что подслово ba устанавливает ту необходимую связь между элементами $\mathcal{H}$-класса J_φ, из-за которой их произведения остаются в J_φ, т. е. $\mathcal{H}$-класс становится максимальной подгруппой. Это подтверждается теоремой 4.13, приводимой ниже, которая суммирует основные выводы этого раздела.

Лемма 4.11. *Пусть φ — конечный слабо примитивный непрерывный эндоморфизм моноида $\widehat{A^*}$. Предположим, что H — максимальная подгруппа J_φ, содержащая некоторый элемент $\operatorname{Im}\varphi^\omega$. Тогда имеется единственная связь ba для φ, такая что $\varphi^\omega(X_\varphi(a,b)) \subseteq H$.*

Доказательство. Пусть a — первая буква, а b — последняя буква элементов из H. Тогда по лемме 4.3 и её двойственному аналогу a — первая буква в $\varphi^\omega(a)$, а b — последняя буква в $\varphi^\omega(b)$. Поскольку H — группа, ba является подсловом из J_φ, что означает, что ba является связью для φ. Так как H содержит некоторый элемент вида $\varphi^\omega(u)$, который начинается с a и заканчивается на b, H является пересечением $\mathcal{R}$-класса $\varphi^\omega(a)$ и $\mathcal{L}$-класса $\varphi^\omega(b)$. Значит, каждый элемент вида $\varphi^\omega(v)$, где $v \in X_\varphi(a,b)$, принадлежит H. Это доказывает существование связи. Единственность следует из того, что, поскольку ba является связью, такой что $\varphi^\omega(X_\varphi(a,b)) \subseteq H$, буква a должна быть первой буквой, а буква b — последней буквой элемента из H. □

Поскольку имеется по крайней мере одна максимальная подгруппа в J_φ, в которой встречается нетривиальный образ $\operatorname{Im}\varphi^\omega$, по утверждению 1 предложения 4.8 мы получаем следующий результат.

Следствие 4.12. *Каждый конечный слабо примитивный непрерывный эндоморфизм моноида $\widehat{A^*}$ имеет по крайней мере одну связь.* □

Предполагая теперь, что φ — специальный эндоморфизм, мы получим более точное утверждение.

Теорема 4.13. *Пусть φ — специальный конечный слабо примитивный непрерывный эндоморфизм моноида $\widehat{A^*}$.*

1. *Пусть H — максимальная подгруппа J_φ, такая что $H \cap \operatorname{Im}\varphi^\omega \neq \varnothing$. Тогда имеется связь ba для φ, такая что $H = \overline{\langle\varphi^\omega(X_\varphi(a,b))\rangle}$.*
2. *Пусть ba является связью для φ. Тогда $\overline{\varphi^\omega(X_\varphi(a,b))^+}$ является максимальной подгруппой J_φ.*

Доказательство. Для данной связи ba для φ по утверждению (2) предложения 4.8 получаем, что $\overline{\varphi^\omega(X_\varphi(a,b))^+}$ содержится в максимальной подгруппе из J_φ и, следовательно, совпадает с $\overline{\langle\varphi^\omega(X_\varphi(a,b))\rangle}$, так как $x^{\omega-1} = \lim\limits_{n\to\infty} x^{n!-1}$. Если H — максимальная подгруппа и доказано утверждение 1, то утверждение 2 будет следовать из единственности в лемме 4.11. Таким образом, мы поступаем с максимальной подгруппой, как в утверждении 1. Из факта существовании связи из леммы 4.11 мы уже имеем включение $\overline{\langle\varphi^\omega(X_\varphi(a,b))\rangle} \subseteq H$ для связи ba для φ. С другой стороны, из утверждения 2 предложения 4.8 получаем, что $\overline{\langle\varphi^\omega(X_\varphi(a,b))\rangle} = \varphi^\omega(H)$. Наконец, по предложению 4.10 $H = \varphi^\omega(H)$, что доказывает утверждение 1. □

Пусть ba является связью для подстановки φ, удовлетворяющей условиям теоремы 4.13. Максимальная подгруппа J_φ, порождённая как топологическая группа множеством $\varphi^\omega(X_\varphi(a,b))$, называется *максимальной подгруппой, ассоциированной с ba*.

5. Подстановки, G-обратимые в конечном счёте

Мы сохраняем предположения раздела 4, а именно считаем, что φ — конечный слабо примитивный непрерывный эндоморфизм моноида $\widehat{A^*}$, где A — конечный алфавит.

Мы скажем, что слабо примитивная подстановка φ является G-*обратимой в конечном счёте*, если существует эндоморфизм $\psi \in \operatorname{End}\widehat{FG_A}$, такой что $\psi \circ p_{\mathsf{G}} \circ \varphi$ переводит каждый элемент $a \in c(\varphi^\omega)$ в порождающий $p_{\mathsf{G}}(a)$. Если мы возьмём $B = c(\varphi^\omega)$, то φ индуцирует непрерывный эндоморфизм φ' на $\widehat{FG_B}$ так: $\varphi'(b) = p_{\mathsf{G}} \circ \varphi(b)$ для $b \in B$. Отметим, что φ является G-обратимой в конечном счёте тогда и только тогда, когда $(\varphi')^\omega$ является тождественным преобразованием на $\widehat{FG_B}$, или, другими словами, когда φ' имеет обратный элемент в проконечном моноиде $\operatorname{End}\widehat{FG_B}$. В случае, если $B = A$, мы будем также говорить, что φ является G-*обратимой*. Заметим, что если φ и ψ — конечные G-обратимые непрерывные эндоморфизмы, то такой же будет и их композиция $\varphi\psi$.

Без дальнейших пояснений мы будем обозначать через $\widehat{FG_B}$ замкнутую подгруппу $\widehat{FG_A}$, порождённую B. Мы будем также рассматривать моноид A^* как естественно вложенный в $\widehat{FG_A}$, а именно как подмоноид, порождённый A.

Предложение 5.1. *Пусть φ — специальный конечный слабо примитивный непрерывный эндоморфизм моноида $\widehat{A^*}$, и пусть $B = c(\varphi^\omega)$. Предположим, что φ является* G*-обратимым в конечном счёте, и пусть ba — связь для φ с ассоциированной максимальной подгруппой H. Тогда ограничение на H естественной проекции $p_{\mathsf{G}}\colon \widehat{A^*} \to \widehat{FG_A}$ имеет в качестве образа замкнутую подгруппу, порождённую множеством $Y_\varphi(a,b)$.*

Доказательство. Поскольку $X_\varphi(a,b) \subseteq Y_\varphi(a,b)$ и $\varphi^\omega(Y_\varphi(a,b)) \subseteq H$, H также порождена как топологическая группа множеством $\varphi^\omega(Y_\varphi(a,b))$. Обозначим ψ единственный непрерывный эндоморфизм $\widehat{FG_A}$, который переводит каждую букву $a \in A$ в положительное слово $\varphi(a)$. Заметим, что $p_{\mathsf{G}} \circ \varphi = \psi \circ p_{\mathsf{G}}$, откуда следует, что ограничение $p_{\mathsf{G}} \circ \varphi^\omega = \psi^\omega \circ p_{\mathsf{G}}$ на $\widehat{B^*}$ такое же, как если бы мы взяли p_{G}, так как φ является G-обратимым в конечном счёте. Значит, замкнутая подгруппа $\widehat{FG_A}$, задаваемая $p_{\mathsf{G}}(H)$, порождается множеством $Y_\varphi(a,b)$. □

Пусть X — конечное непустое подмножество полугруппы A^+. *Элементарное расщепление*, выполненное над X, состоит в нахождении в X пары различных слов либо вида x, xy, либо вида x, yx и построении множества X', которое можно получить из X заменой xy (соответственно yx) на y. Тогда мы, очевидно, имеем $\langle X\rangle = \langle X'\rangle$ и $X^* \subseteq (X')^*$. Заметим, что $\sum\limits_{x\in X} |x| > \sum\limits_{x'\in X'} |x'|$, поэтому любая последовательность элементарных расщеплений, выполненных над X, должна в конце концов привести к конечному подмножеству Y в A^+, над которым нельзя провести никакое элементарное расщепление, т. е. к Y, которое является конечным бипрефиксным кодом. Кроме того, легко видеть, что преобразование элементарного расщепления локально конфлюэнтно в том смысле, что когда к множеству X применяются два различных преобразования элементарного расщепления, чтобы получить множества X' и X'', то имеется множество Z, которое может быть получено как из X', так и из X'' применением некоторых элементарных расщеплений. Следовательно, имеется единственный бипрефиксный код $\tilde{X}$, который может быть получен из X применением последовательности элементарных расщеплений. Мы назовём его *расщеплённым кодом* множества X. Принимая во внимание факт, что если $w(a_1,\dots,a_n)$ является нетривиальным приведённым групповым словом и мы подставим вместо элементов a_i различные элементы u_i бипрефиксного кода, то групповое слово $w(u_1,\dots,u_n)$ нельзя будет привести к пустому слову, мы получаем следующий результат, равнозначный простому и, вероятно, фольклорному упражнению из комбинаторной теории групп.

Предложение 5.2. *Пусть X — конечное непустое подмножество A^+. Тогда расщепляющий код $\tilde{X}$ — это множество всех свободных порождающих подгруппы $\langle X\rangle$ свободной группы FG_A и $X^* \subseteq \tilde{X}^*$.* □

Сейчас мы уже готовы рассмотреть один из основных результатов этой работы.

Теорема 5.3. *Пусть φ — специальный слабо примитивный непрерывный эндоморфизм моноида $\widehat{A^*}$. Предположим, что φ G-обратим в конечном счёте, и пусть ba является связью для φ, ассоциированной с максимальной подгруппой H. Тогда отображение $\chi\colon H \to \widehat{FG_A}$, полученное ограничением естественной проекции $p_{\mathsf{G}}\colon \widehat{A^*} \to \widehat{FG_A}$, является изоморфизмом из H на замкнутую подгруппу, порождённую множеством $Y_\varphi(a,b)$, которая является конечно порождённой свободной проконечной группой с множеством свободных порождающих $\widetilde{Y_\varphi(a,b)}$.*

Доказательство. Согласно предложению 5.1 и его доказательству $p_{\mathsf{G}}(\varphi^\omega(u)) = u$ для $u \in A^*$. Пусть $K = \langle \widetilde{Y_\varphi(a,b)} \rangle$. По предложению 5.2 K является свободной группой на множестве $\widetilde{Y_\varphi(a,b)}$. Из результата Кулбуа, Сапира и Вейля [15, теорема 1.1], применённого к псевдомногообразию G всех конечных групп, замыкание $\overline{K}$ группы K в $\widehat{FG_A}$ является свободной проконечной группой на $\widetilde{Y_\varphi(a,b)}$. Это уже обеспечивает то, что $\operatorname{Im}\chi$ — конечно порождённая свободная проконечная группа. Осталось показать, что χ инъективно. Для этого достаточно показать, что H порождается как замкнутая подгруппа элементами, которые отображением χ переводятся в $\widetilde{Y_\varphi(a,b)}$.

Незначительной трудностью в доказательстве в этом месте является то, что $\varphi^\omega(v)$ может не принадлежать H для $v \in \widetilde{Y_\varphi(a,b)}$. Чтобы обойти эту трудность, мы должны предъявить модифицированное псевдослово v', такое что $\varphi^\omega(v') \in H$ и $\chi(\varphi^\omega(v')) = v$. Это просто сделать, имитируя в группе H последовательность сокращений, ведущих от множества $Y_\varphi(a,b)$ к $\widetilde{Y_\varphi(a,b)}$, используя операцию возведения в степень $\omega - 1$. Более точно, предположим, что X — множество порождающих H как топологической группы и что x и y — два различных элемента X. Тогда, заменяя y на $x^{\omega-1}y$ или на $yx^{\omega-1}$, получим другое подмножество H, которое остаётся порождающим для H как топологической группы. Нужный результат следует из того, что χ является групповым гомоморфизмом и что возведение в степень $\omega - 1$ в $\widehat{FG_A}$ совпадает с обращением. □

Напомним понятие циклического кода из [13]. Подмножество C полугруппы A^+ является *циклическим кодом*, если всякий раз, когда $p \in A^*$, $s \in A^+$, $c_1, \ldots, c_m, d_1, \ldots, d_n \in C$, $sc_2 \ldots c_m p = d_1 \ldots d_n$ и $c_1 = ps$, мы имеем $m = n$, $p = 1$ и $c_i = d_i$ $(1 \leqslant i \leqslant n)$. Это свойство эквивалентно тому, что подмоноид C^* свободного моноида A^* является *очень строгим* в том смысле, что $uv, vu \in C^*$ влечёт $u, v \in C^*$ и C является минимальным множеством порождающих C^*. Мы скажем, что $\varphi \in \operatorname{End}\widehat{A^*}$ является *циклическим кодированием*, если $\varphi|_B$ инъективно и $\varphi(B)$ — циклический код, где $B = c(\varphi^\omega)$.

Предложение 5.4. *Пусть φ — конечный непрерывный G-обратимый в конечном счёте эндоморфизм моноида $\widehat{A^*}$. Тогда φ будет циклическим кодированием.*

Доказательство. Пусть $B = c(\varphi^\omega)$. Из предложения 5.2 следует, что $\widetilde{\varphi(B)} = B$, и поэтому имеется последовательность элементарных расщеплений, начинающаяся с $\varphi(B)$, которая заканчивается в множестве B, которое, конечно, является циклическим кодом. Идея доказательства — проследить элементарные расщепления в обратном направлении и показать, что на каждой стадии получается циклический код. Чтобы доказать этот факт, мы используем хорошо известный результат теории кодирования, а именно что композиция двух циклических кодов снова является циклическим кодом [13, предложение 1.9]. Действительно, если $X = \{x_1, x_2, \ldots, x_n\}$ — циклический код, то множество $\{x_1x_2, x_2, \ldots, x_n\}$ получено композицией кода $\{d_1d_2, d_2, \ldots, d_n\}$ над алфавитом $D = \{d_1, d_2, \ldots, d_n\}$ с кодом X. Аналогичное утверждение справедливо для двойственной конструкции $\{x_2x_1, x_2, \ldots, x_n\}$. Поэтому достаточно показать, что код $Z = \{d_1d_2, d_2, \ldots, d_n\}$ (вместе с его двойственным) является циклическим кодом, что соответствует первому шагу анонсированной процедуры обратного отслеживания элементарных расщеплений.

Поскольку Z является даже префиксным кодом, достаточно показать, что Z^* — очень строгий подмоноид D^*. В самом деле, если $u, v \in D^*$ и $uv, vu \in Z^*$, то $u, v \in Z^*$, так как, например, если в u не за каждой буквой d_1 следует d_2, то то же самое выполняется и для vu, а это противоречит тому, что $vu \in Z^*$. □

Дальнейшее есть вариация некоторых сходных результатов, которые могут быть найдены в литературе по алгебраической теории кодирования при различных определениях понятия запаздывания [13, § VII.2]. Поскольку кажется, что в точности то определение языка ограниченного запаздывания, которое было использовано в этой статье, ещё не встречалось в литературе, мы ради полноты картины приведём и доказательства.

Лемма 5.5. *Каждый конечный циклический код имеет ограниченное запаздывание.*

Доказательство. Пусть C — конечный циклический код над алфавитом A. Тогда имеется оценка сверху для числа различных перекрытий между словами в C. Под перекрытием понимается разложение вида $xc = c'y$, где $c, c' \in C$, $x \in A^*$, $y \in A^+$ и $|x| < |c'|$, как изображено на рис. 4. Значит, при условии, что

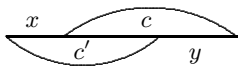


Рис. 4. Перекрытие между двумя кодовыми словами

сумма $m + n$ достаточно велика, если имеются два разложения

$$uc_1 \ldots c_m v = c'_1 \ldots c'_n, \tag{5.1}$$

где $c_i, c'_j \in C$, то при рассмотрении перекрытий между подсловами c_i и c'_j должно быть по крайней мере два равных перекрытия, что ведёт к равенствам следующего вида: $sc_ic_{i+1} \ldots c_{i+r-1}p = c'_jc'_{j+1} \ldots c'_{j+t}$ и $ps = c_{i+r}$, где $s \neq 1$. Из того, что

C — циклический код, следует, что $p = 1$. Это означает, что равенство (5.1) является приводимым. Другой тип равенств, содержащихся в определении языка ограниченного запаздывания, обрабатывается аналогично. □

Следствие 5.6. *Пусть φ — конечный* G*-обратимый в конечном счёте слабо примитивный непрерывный эндоморфизм моноида $\widehat{A^*}$. Тогда φ является специальным.*

Доказательство. Утверждение непосредственно следует из предложения 5.4 и леммы 5.5. □

Теперь мы можем упростить формулировку теоремы 5.3, устранив из неё явное упоминание технического условия, что эндоморфизм φ специальный.

Следствие 5.7. *Пусть φ — конечный* G*-обратимый в конечном счёте слабо примитивный непрерывный эндоморфизм моноида $\widehat{A^*}$. Тогда максимальные подгруппы из J_φ — это конечно порождённые свободные проконечные группы.*

Доказательство. Согласно следствию 5.6 φ является специальным. По теореме 5.3 имеется максимальная подгруппа H из J_φ, такая что ограничение на H естественной проекции $p_{\mathsf{G}}\colon \widehat{A^*} \to \widehat{FG_A}$ является вложением, которое отображает H на конечно порождённую свободную проконечную группу. □

Другое следствие теоремы 5.3 — это следующий результат, для которого мы не нашли прямого доказательства.

Следствие 5.8. *Пусть φ — конечный* G*-обратимый в конечном счёте слабо примитивный непрерывный эндоморфизм моноида $\widehat{A^*}$, и пусть ba — связь для φ. Тогда имеется следующее равенство подгрупп в FG_A: $\langle X_\varphi(a,b)\rangle = \langle Y_\varphi(a,b)\rangle$, или, эквивалентно, $\widetilde{X_\varphi(a,b)} = \widetilde{Y_\varphi(a,b)}$.*

Доказательство. Пусть H — максимальная подгруппа, которая содержит $\varphi^\omega(X_\varphi(a,b))$. Согласно утверждению (2) теоремы 4.13 H порождается как топологическая группа множеством $\varphi^\omega(X_\varphi(a,b))$. Пусть $\chi\colon H \to \widehat{FG_A}$ — ограничение естественной проекции $p_{\mathsf{G}}\colon \widehat{A^*} \to \widehat{FG_A}$ на H. По теореме 5.3 мы получаем равенство $\chi(H) = \overline{\langle Y_\varphi(a,b)\rangle}$. С другой стороны, так как χ — непрерывный гомоморфизм и $H = \overline{\varphi^\omega(X_\varphi(a,b))^+}$, мы также имеем равенство $\chi(H) = \overline{\langle X_\varphi(a,b)\rangle}$. Это показывает, что

$$\overline{\langle X_\varphi(a,b)\rangle} = \overline{\langle Y_\varphi(a,b)\rangle}. \tag{5.2}$$

Остаётся воспользоваться теоремой M. Холла [16], согласно которой конечно порождённые подгруппы $\langle X_\varphi(a,b)\rangle$ и $\langle Y_\varphi(a,b)\rangle$ группы FG_A замкнуты в проконечной топологии и имеют одинаковое замыкание ввиду (5.2). □

Мы завершаем этот раздел двумя примерами. Первый показывает, что следствие 5.8 может не выполняться, если опустить предположение, что эндоморфизм φ G-обратим в конечном счёте. Второй пример иллюстрирует вычисление максимальной подгруппы. В обоих случаях мы полагаем $A = \{a, b, c\}$.

Пример 5.9. Пусть φ — подстановка, заданная так: $\varphi(a) = bac$, $\varphi(b) = cba$, $\varphi(c) = acb$. Заметим, что это примитивная подстановка и ab является связью для φ. Используя лемму 4.5, можно вычислить, что

$$X_\varphi(b,a) = \{bacacbacbcba, bacacbbacacbcba, bacacbbacacbcbaacbcba,\\ bacacbbacacbcbacba, bacacbcba, bacacbcbaacbcba,\\ bacbacacbcbaacbcba, baccba\},$$

из чего следует, что $Y_\varphi(b,a)$ содержит элементы ba, bba, $bcba$, которые порождают свободную группу FG_A. С другой стороны, $\widetilde{X_\varphi(b,a)} = \{acb, bac, cba\}$, что совпадает с $\varphi(A)$.

Пример 5.10. Рассмотрим непрерывный эндоморфизм моноида $\widehat{A^*}$, определённый так: $\varphi(a) = bcac$, $\varphi(b) = bcacbc$, $\varphi(c) = cbcbcac$. Небольшое вычисление, использующее лемму 4.5, показывает, что cb является связью для φ и что $X_\varphi(b,c) = \{bc, bcc, bcac, bcacc\}$. Значит, $\widetilde{X_\varphi(b,c)} = \{a,b,c\}$. Согласно теореме 5.3 и её доказательству максимальная подгруппа, содержащая $\varphi^\omega(bc)$, — это свободная проконечная группа, свободно порождённая множеством

$$\Big\{\varphi^\omega\Big(((bc)^\omega c)^{\omega-1}\cdot\big(bc((bc)^\omega c)^{\omega-1}\big)^{\omega-1}\cdot bcac\cdot((bc)^\omega c)^{\omega-1}\Big),\\ \varphi^\omega\big(bc\cdot((bc)^\omega c)^{\omega-1}\big), \varphi^\omega\big((bc)^{\omega-1}\cdot bcc\big)\Big\}.$$

Пример 5.10 иллюстрирует вычисление специфической максимальной подгруппы $\mathcal{J}$-класса, ассоциированной с конечной слабо примитивной подстановкой. Это вычисление эффективно в том смысле, что связь ba и ассоциированное с ней конечное множество слов $Y_\varphi(a,b)$ могут быть найдены эффективно. В случае, если φ — G-обратимый в конечном счёте эндоморфизм, вычисление расщеплённого кода $\widetilde{Y_\varphi(a,b)}$ сводится к описанию множества свободных порождающих (в смысле топологических групп) максимальной подгруппы H из J_φ, содержащей $\varphi^\omega(Y_\varphi(a,b))$. Кроме того, принимая во внимание, что в проконечном моноиде выполняется равенство $u^{\omega-1} = \lim\limits_{n\to\infty} u^{n!-1}$, мы заключаем, что полученные свободные порождающие H определяют эффективно вычислимые «неявные операции». Обсуждение вопросов вычислимости и сложности можно найти в [10] (см. там предложение 4.5 и последующие замечания).

6. $\mathcal{J}$-классы Штурма и Арну—Рози, порождённые подстановками

Этот раздел посвящён некоторым важным специальным случаям применения теоремы 5.3, в которых возможно более точно оценить число свободных

порождающих максимальных подгрупп $\mathcal{J}$-классов, ассоциированных с конечным G-обратимым в конечном счёте слабо примитивным непрерывным эндоморфизмом φ моноида $\widehat{A^*}$. Результаты этого раздела уже были опубликованы без доказательств в [7].

Первое простое приложение получается при рассмотрении подстановочного сдвигового пространства[1] Штурма. Такие сдвиговые пространства получаются итерированием примитивных эндоморфизмов φ конечного моноида $\{a,b\}^*$, которые являются G-обратимыми. Эти эндоморфизмы также известны как *подстановки Штурма*. Конечные подслова из J_φ должны быть *сбалансированы* в том смысле, что число появлений данной буквы в подсловах одинаковой длины не может отличаться более чем на 1 и число подслов длины n равно $n+1$ [18, глава 2]. Из этого следует, что слово ba является подсловом и $X_\varphi(a,b)$ содержит ровно два элемента: в случае, если aa не является подсловом, элементами $X_\varphi(a,b)$ будут ab^n и ab^{n+1} для некоторого $n \geqslant 1$; в случае, если bb не является подсловом, элементами будут a^nb и $a^{n+1}b$ для некоторого $n \geqslant 1$. В обоих случаях $X_\varphi(a,b)$ порождает свободную группу $FG_{\{a,b\}}$, поэтому теорема 5.3 применима, когда ba является связью для φ. Случай, когда ab является связью, двойствен предыдущему. Случай, когда одно из слов aa или bb является связью, существенно легче. В самом деле, скажем, в случае, когда aa является связью, $Y_\varphi(a,a)$ содержит как a, так и слово aba (так как в противном случае множество конечных подслов J_φ не было бы сбалансированным), что показывает, что $Y_\varphi(a,a)$ порождает свободную группу $FG_{\{a,b\}}$.

Следствие 6.1. *Пусть φ — подстановка Штурма. Тогда максимальные подгруппы моноида J_φ являются свободными проконечными группами с двумя свободными порождающими.* □

Мы также уже анонсировали в [7], что отсюда следует, что для максимального регулярного $\mathcal{J}$-класса моноида $\widehat{\{a,b\}^*}$, ассоциированного с произвольным сдвиговым пространством Штурма над алфавитом $\{a,b\}$, максимальные подгруппы также являются свободными проконечными группами с двумя свободными порождающими.

Обобщение сдвигового пространства Штурма, предложенное Арну и Рози (см. [14]), может быть определено следующим образом. Рассмотрим сначала гомоморфизм *Арну—Рози*

$$\rho\colon \widehat{A^*} \to \operatorname{End} \widehat{A^*},$$
$$w \mapsto \rho_w,$$

определённый следующей формулой для $a, b \in A$:

[1] Под *сдвиговым пространством* мы понимаем символическую динамическую систему над конечным алфавитом A, т. е. замкнутое подмножество $A^{\mathbb{Z}}$, стабильное относительно всех сдвигов начала. Сдвиговое пространство называется *подстановочным*, если оно порождается итерацией подстановки в смысле, описанном подробно в [14].

$$\rho_a(b) = \begin{cases} a, & \text{если } a = b, \\ ab & \text{иначе.} \end{cases}$$

Мы скажем, что слово $u \in A^*$ имеет *полное содержание*, если $c(u) = A$.

Лемма 6.2. *Пусть $u \in A^*$ — конечное слово с полным содержанием.*

1. *Отображение ρ_u является конечным* G*-обратимым примитивным непрерывным эндоморфизмом моноида $\widehat{A^*}$.*
2. *Существует связь ba для ρ_u, такая что множество $Y_{\rho_u}(a, b)$ порождает свободную группу FG_A.*

Доказательство.

1. Так как каждое отображение ρ_a, где $a \in A$, является G-обратимым, таким же будет и отображение ρ_u. Чтобы доказать первое утверждение, осталось показать, что ρ_u является примитивным. Это следует из того, что для $u, v \in A^*$

$$c(\rho_u(v)) = c(u) \cup c(v), \tag{6.1}$$

что легко доказать индукцией по длине u.

2. Пусть a — первая буква в слове u. Тогда $\operatorname{Im} \rho_{u^n} \subseteq \operatorname{Im} \rho_a$ и, так как каждое конечное подслово $\rho_u^\omega(a) = \rho_{u^\omega}(a)$ является подсловом всех слов вида $\rho_{u^{n!}}(a)$ для достаточно больших n, такое подслово должно быть подсловом $\rho_a(v)$ для некоторого слова v. Итак, $\operatorname{Im}(\rho_a|_{A^*})$ — подмоноид моноида A^*, порождённый словами вида ab, где $b \in A \setminus \{a\}$, и буквой a. Кроме того, согласно формуле (6.1), если $u = au'$, то a появляется в $\rho_{u'u^n}(a)$ следом за другой буквой для всех $n \geqslant 1$, и поэтому aa является подсловом $\rho_{u^n}(a)$ для $n > 1$. Отметим также, что $\rho_{u^n}(a)$ начинается и заканчивается буквой a. Значит, подслово aa является связью для ρ_u.

Осталось показать, что множество $Y_{\rho_u}(a, a)$ порождает свободную группу FG_A. По определению множества $Y_{\rho_u}(a, a)$, так как его элементы должны быть подсловами слов, полученных из a и двубуквенных слов вида ab ($b \in A \setminus \{a\}$), $Y_{\rho_u}(a, a)$ содержит как букву a, так и все слова вида aba, где $b \in A \setminus \{a\}$. Из таких слов посредством вычёркивания буквы a мы получим все другие буквы из A, значит, $Y_{\rho_u}(a, a)$ порождает FG_A. □

Применяя теорему 5.3, мы получим следующий результат, из которого может быть выведено следствие 6.1 [7].

Следствие 6.3. *Пусть $u \in A^*$ — слово с полным содержанием. Тогда максимальные подгруппы максимального регулярного $\mathcal{J}$-класса J_{ρ_u} — это свободные проконечные группы с $|A|$ свободными порождающими.*

Сдвиговые пространства, соответствующие $\mathcal{J}$-классам, появившиеся в следствии 6.3, известны как *сдвиговые пространства Арну—Рози* (порождённые подстановками) [7, 14, 18]. Они представляют собой обобщение сдвиговых пространств, порождённых подстановками Штурма. Более подробно, сдвиговое пространство (или псевдослово) над конечным алфавитом A называется сдвиговым

пространством Арну—Рози, если для каждого $n \geqslant 1$ оно имеет ровно одно правое специальное и одно левое специальное подслово длины n, каждое степени $|A|$. Здесь подслово u называется *правым специальным степени* d, если имеется в точности $d > 1$ букв $a \in A$, таких что ua тоже является подсловом, а *левое специальное подслово степени* d определяется двойственным образом. Как уже отмечалось в [7], из результата о правых бесконечных словах, т. е. словах из $A^{\mathbb{N}}$, следует, что каждое псевдослово Арну—Рози $\mathcal{J}$-эквивалентно некоторому псевдослову вида $\rho_v(a)$, где $v \in \widehat{A^*}$, в котором каждая буква встречается неограниченное число раз в конечных префиксах v [12, 14]. Фактически последовательности конечных префиксов v, т. е. правого бесконечного слова, достаточно, чтобы определить $\mathcal{J}$-класс. Сдвиговые пространства Арну—Рози, порождённые подстановками, соответствуют случаю, когда рассматриваемые правые бесконечные слова являются периодическими.

В [7] обрисовано, как расширить следствие 6.3 на максимальные подгруппы $\mathcal{J}$-классов, ассоциированных с произвольными сдвиговыми пространствами Арну—Рози, не обязательно порождёнными бесконечной итерацией конечного эндоморфизма.

7. Некоторые примеры

Мы рассмотрим в этом разделе несколько примеров, чтобы проиллюстрировать то, что происходит за пределами тех красивых классов, которые изучались в разделах 5 и 6, когда общая проблема вычисления $\mathcal{J}$-максимальной подгруппы в $\widehat{A^*}$ остаётся открытой.

Пример 7.1. Пусть $A = \{a, b, c\}$, и пусть отображение $\varphi \in \operatorname{End} \widehat{A^*}$ определено так: $\varphi(a) = bac$, $\varphi(b) = cbac$, $\varphi(c) = bacb$. Тогда bc является подсловом слова $\varphi^2(b) = bacbcbacbacbacb$ и, следовательно, подсловом φ^ω, применённого к любой букве, так как подстановка φ примитивна. Небольшие вычисления, использующие лемму 4.5, показывают, что bc является связью для φ и что $X_\varphi(c, b) = \{cbacbacb, cbacbacbacb\}$, следовательно, $Y_\varphi(c, b) = \{(cba)^n cb\colon n = 0, 1, 2, 3\}$. Поэтому подгруппа FG_A, порождённая $Y_\varphi(c, b)$, порождена также $\{a, cb\}$. Заметим, что эндоморфизм φ G-обратим. Следовательно, по теореме 5.3 максимальные подгруппы J_φ являются проконечными группами на двух порождающих.

Пример 7.2. Пусть $A = \{a, b\}$. Рассмотрим непрерывный эндоморфизм $\widehat{A^*}$, определённый правилами $\varphi(a) = ab$ и $\varphi(b) = a^3b$. Заметим, что φ — - это конечная примитивная подстановка, не являющаяся G-обратимой. Мы утверждаем, что максимальная подгруппа J_φ не будет свободной проконечной группой.

Согласно [10, предложение 4.3] псевдослова $\varphi^\omega(a)$ и $\varphi^\omega(b)$ лежат в одной максимальной подгруппе H моноида J_φ. Отсюда $\operatorname{Im} \varphi^\omega \subseteq H$. Заметим, что φ — это префиксный код с запаздыванием 1 и, следовательно, φ является специальным эндоморфизмом. По предложению 4.10 мы заключаем, что $H = \operatorname{Im} \varphi^\omega$. С другой стороны, по теореме 4.13 максимальная подгруппа H порождается как

замкнутая подгруппа множеством $\varphi^\omega(X_\varphi(a,b))$. Поскольку $\varphi(A^*) = \{ab, a^3b\}$, легко понять, что $X_\varphi(a,b) = \{ab, a^3b\}$. Поэтому H порождается как замкнутая подгруппа множеством $\{\varphi^\omega(ab), \varphi^\omega(a^3b)\}$.

Если бы проконечная группа H была свободной с двумя порождающими, она также была бы свободной с любыми двумя порождающими. В частности, H была бы свободно порождённой как проконечная группа как парой $\varphi^\omega(ab)$, $\varphi^\omega(a^3b)$, так и парой $\varphi^\omega(a)$, $\varphi^\omega(b)$. Следовательно, имелся бы непрерывный гомоморфизм $\psi\colon H \to \mathbb{Z}/2\mathbb{Z}$, который переводил бы как $\varphi^\omega(a)$, так и $\varphi^\omega(b)$ в 1 (1 означает здесь порождающий элемент аддитивной группы $\mathbb{Z}/2\mathbb{Z}$). Тогда ψ переводит как $\varphi^\omega(ab)$, так и $\varphi^\omega(a^3b)$ в $0 = 1+1$, что противоречит уже установленному факту, что два псевдослова порождают плотную подгруппу в H. Поэтому H не является свободной группой с двумя порождающими.

Чтобы завершить доказательства того, что H не является свободной проконечной группой, достаточно показать, что она не является проциклической группой. Для того чтобы установить это свойство, рассмотрим непрерывный гомоморфизм $\theta\colon \widehat{A^*} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, который переводит a в $(1,0)$, а b в $(0,1)$, где 1 означает обычный порождающий элемент $\mathbb{Z}/3\mathbb{Z}$. Тогда легко видеть, что $\theta(\varphi^n(a))$ и $\theta(\varphi^n(b))$ равны соответственно первому и второму столбцам матрицы M^n, вычисленной над полем $\mathbb{Z}/3\mathbb{Z}$, где

$$M = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Из того, что M^3 — единичная матрица, следует, что $\theta(\varphi^\omega(a)) = (1,0)$ и $\theta(\varphi^\omega(b)) = (0,1)$. Значит, H не является проциклической группой, так как имеет нециклическую конечную группу в качестве непрерывного гомоморфного образа. Это завершает доказательство того, что максимальная подгруппа H в J_φ не является свободной проконечной группой.

Предыдущий пример, вероятно, является первым примером максимальной подгруппы конечно порождённого свободного проконечного моноида, не являющейся свободной проконечной.

Пример 7.3. Пусть $A = \{a, b\}$, и пусть непрерывный эндоморфизм φ моноида $\widehat{A^*}$ определён так: $\varphi(a) = ab$ и $\varphi(b) = ba$. Это хорошо известная подстановка Пруэ—Туэ—Морса [14]. Рассмотрим $\mathcal{J}$-класс J_φ элемента $\alpha = \varphi^\omega(a)$. Заметим, что a^2 является связью для φ, поэтому α лежит в максимальной подгруппе H. Простое вычисление показывает, что $X_\varphi(a,a) = \{a, aba, ab^2a\}$. Эндоморфизм φ является кодом не с ограниченным, а с относительно ограниченным запаздыванием, поэтому является специальным. Следовательно, согласно общей теории, H — замыкание подгруппы, порождённой $\alpha = \varphi^\omega(a)$, $\beta = \varphi^\omega(aba)$ и $\gamma = \varphi^\omega(ab^2a)$. Мы утверждаем, что α, β, γ не являются свободными порождающими H, откуда следует, что группа H не является свободной проконечной группой с тремя порождающими, хотя она может быть свободной проконечной группой с меньшим числом порождающих. Чтобы доказать это

утверждение, рассмотрим непрерывный эндоморфизм φ^2 моноида $\widehat{A^*}$, определяемый так: $\varphi^2(a) = abba$ и $\varphi^2(b) = baab$. Поскольку элементы H имеют вид $\varphi^\omega(ava)$ для некоторого псевдослова v, их образы при действии φ^2 будут иметь вид $\varphi^\omega(abbav'abba)$. Так как буква принадлежит J_φ по предложению 4.2, она принадлежит и H. Отсюда $\varphi^2(H) \subseteq H$. С другой стороны, мы имеем

$$\varphi^\omega(ava) = \varphi^2(\varphi^{\omega-2}(\varphi^\omega(ava))) = \varphi^2\Big(\lim_{n\to\infty} \varphi^{n!-2}(\varphi^\omega(ava))\Big).$$

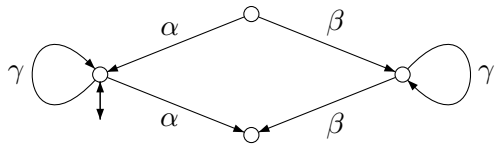
Так как по предположению $\varphi^\omega(ava)$ принадлежит H, $\varphi^{n!-2}$ является степенью φ^2 для $n \geqslant 3$, $\varphi^2(H) \subseteq H$ и H замкнуто, мы заключаем, что $H = \varphi^2(H)$. Из того, что эндоморфизм φ^2 инъективен согласно [19], следует, что φ^2 индуцирует непрерывный автоморфизм H. Следовательно, если бы H свободно порождалась как проконечная группа псевдословами α, β, γ, то она бы свободно порождалась их образами при действии отображения φ^2, которые мы сейчас вычислим. Ясно, что $\varphi^2(\alpha) = \gamma$. С другой стороны,

$$\varphi^2(\beta) = \varphi^\omega(abba\,baab\,abba) = \\ = \varphi^\omega(abba \cdot a^{\omega-1} \cdot aba \cdot aba \cdot a^{\omega-1} \cdot abba) = \gamma\alpha^{-1}\beta^2\alpha^{-1}\gamma$$

и, аналогично,

$$\varphi^2(\gamma) = \varphi^\omega(abba\,baab\,baab\,abba) = \\ = \varphi^\omega(abba \cdot a^{\omega-1} \cdot aba \cdot abba \cdot aba \cdot a^{\omega-1} \cdot abba) = \gamma\alpha^{-1}\beta\gamma\beta\alpha^{-1}\gamma.$$

Таким образом, φ^2 переводит подгруппу H_0, (дискретно) порождённую α, β, γ, в её подгруппу. Вычисляя минимальный инверсный автомат, распознающий эту подгруппу, получаем следующий автомат:



Следовательно, множество $\varphi^2\{\alpha, \beta, \gamma\}$ порождает собственную подгруппу K группы H_0. Предполагая, что H свободно порождена как проконечная группа псевдословами α, β, γ, получаем, что H_0 порождена как дискретная группа этими же элементами. Отсюда по теореме М. Холла [16] следует, что K замкнута в проконечной топологии H_0, которая индуцирована топологией H. Получили противоречие, так как, как уже было показано, множество $\varphi^2\{\alpha, \beta, \gamma\}$ порождаёт плотную подгруппу в H. Поэтому H не порождена свободно элементами α, β, γ.

Автор хотел бы поблагодарить Альфредо Кошту, Кунитаку Шоджи и Бенджамина Стейнберга за полезные обсуждения некоторых идей, отражённых в этой работе. Он благодарен также Альфредо Коште и Бенджамину Стейнбергу

за их комментарии по поводу предыдущих версий этой статьи и М. В. Волкову за ссылки на работы Виландта и Марковского.

Эта работа была поддержана, в частности, Фондом науки и технологии (FCT) центра математики Университета Порту и одобренным POCTI проектом POCTI/32817/MAT/2000, который частично финансируется Фондом европейского сообщества FEDER. Работа была закончена во время визита автора в лабораторию оснований и приложений алгоритмической информатики (LIAFA) Университета Дени Дидро (Париж-7), которой автор благодарен за гостеприимство. Научный отпуск автора был поддержан стипендией FCT.

Литература

[1] Almeida J. Some algorithms on the star operation applied to finite languages // Semigroup Forum. — 1984. — Vol. 28. — P. 187—197.

[2] Almeida J. Finite Semigroups and Universal Algebra. — Singapore: World Scientific, 1995.

[3] Almeida J. Dynamics of implicit operations and tameness of pseudovarieties of groups // Trans. Amer. Math. Soc. — 2002. — Vol. 354. — P. 387—411.

[4] Almeida J. Finite semigroups: An introduction to a unified theory of pseudovarieties // Semigroups, Algorithms, Automata and Languages / G. M. S. Gomes, J.-E. Pin, P. V. Silva, eds. — Singapore: World Scientific, 2002. — P. 3—64.

[5] Almeida J. Profinite semigroups and applications. — Tech. Rep. CMUP 2003-33. — Univ. Porto, 2003.

[6] Almeida J. Profinite structures and dynamics // CIM Bulletin. — 2003. — Vol. 14. — P. 8—18.

[7] Almeida J. Symbolic dynamics in free profinite semigroups. — No. 1366 in RIMS Kokyuroku, Kyoto, Japan, April 2004. — P. 1—12.

[8] Almeida J., Steinberg B. On the decidability of iterated semidirect products and applications to complexity // Proc. London Math. Soc. — 2000. — Vol. 80. — P. 50—74.

[9] Almeida J., Steinberg B. Syntactic and global semigroup theory, a synthesis approach // Algorithmic Problems in Groups and Semigroups / J. C. Birget, S. W. Margolis, J. Meakin, M. V. Sapir, eds. — Birkhäuser, 2000. — P. 1—23.

[10] Almeida J., Volkov M. V. Subword complexity of profinite words and subgroups of free profinite semigroups // Internat. J. Algebra Comput. — To appear.

[11] Almeida J., Weil P. Relatively free profinite monoids: An introduction and examples // Semigroups, Formal Languages and Groups / J. B. Fountain, ed. — Vol. 466. — Dordrecht: Kluwer Academic, 1995. — P. 73—117.

[12] Berstel J. Recent results on extensions of Sturmian words // Internat. J. Algebra Comput. — 2002. — Vol. 12. — P. 371—385.

[13] Berstel J., Perrin D. Theory of Codes. — New York: Academic Press, 1985.

[14] Introduction to Finite Automata and Substitution Dynamical Systems / V. Berthé, S. Ferenczi, C. Mauduit, A. Siegel, eds. — 2001. — `http://iml.univ-mrs.fr/editions/preprint00/book/prebookdac.html`.

[15] Coulbois T., Sapir M., Weil P. A note on the continuous extensions of injective morphisms between free groups to relatively free profinite groups // Publ. Mat. — 2003. — Vol. 47. — P. 477—487.

[16] Hall M. A topology for free groups and related groups // Ann. Math. — 1950. — Vol. 52. — P. 127—139.

[17] Lallement G. Semigroups and Combinatorial Applications. — New York: Wiley, 1979.

[18] Lothaire M. Algebraic Combinatorics on Words. — Cambridge: Cambridge University Press, 2002.

[19] Margolis S., Sapir M., Weil P. Irreducibility of certain pseudovarieties // Comm. Algebra. — 1998. — Vol. 26. — P. 779—792.

[20] Markowsky G. Bounds on the index and period of a binary relation on a finite set // Semigroup Forum. — 1976. — Vol. 13. — P. 253—259.

[21] Queffélec M. Substitution Dynamical Systems — Spectral Analysis. — Lect. Notes Math. Vol. 1294. — Berlin: Springer, 1987.

[22] Spehner J.-C. Quelques constructions et algorithmes relatifs aux sous-monoïdes d'un monoïde libre // Semigroup Forum. — 1975. — Vol. 9. — P. 334—353.

[23] Weil P. Profinite methods in semigroup theory // Internat. J. Algebra Comput. — 2002. — Vol. 12. — P. 137—178.

[24] Wielandt H. Unzerlegbare, nicht negative Matrizen // Math. Z. — 1950. — Vol. 52. — P. 642—648.