О связи специальных бинарных отношений с условиями коммутирования языков. Часть I. Делители в глобальном надмоноиде

Б. Ф. Мельников

***Аннотация*—В статье рассматриваются различные утверждения, описывающие связь специальных бинарных отношений (а именно – исследованных в нескольких наших предыдущих работах бинарных отношениях покрытия и эквивалентности в бесконечности) с условиями коммутирования языков. Обобщая можно сказать, что рассматриваются просто формулируемые свойства, связанные с применением операции произведения (конкатенации) формальных языков – причём не обязательно (но обычно) языков конечных. Среди этих проблем – исследование условий равенства степеней двух языков. Доказывается, например, что в случае префиксных языков такое равенство равносильно наличию у рассматриваемых множеств общего корня, определяемого для операции конкатенации обычным образом.**

В начале статьи приводятся несколько вспомогательных утверждений, связанных с возможным выбором для заданного языка его левого делителя. Далее особо рассматриваются те из полученных результатов про левый делитель, которые удачно переформулируются, если рассматриваемые в утверждениях языки могут быть получены в результате действия каких-либо морфизмов. Далее рассматриваются условия наличия в глобальном надмоноиде общего корня для некоторых двух его элементов.

После этого рассматриваются различные следствия условия возможного коммутирования двух языков: сначала в общем случае, а затем – при наличии условия префиксности рассматриваемых языков. В заключении статьи приводятся различные интересные примеры, а также формулируются пока не решённые задачи.

***Ключевые слова*—формальные языки, свободный моноид, надмоноиды, итерации языков, коммутирование, алгоритмы.**

I. ВВЕДЕНИЕ И МОТИВАЦИЯ

В статье рассматриваются различные утверждения, описывающие связь специальных бинарных отношений (а именно – исследованных в наших предыдущих работах бинарных отношениях покрытия $\trianglelefteq$ и эквивалентности в бесконечности $\Leftrightarrow$) с условиями коммутирования языков. Обобщая можно сказать, что рассматриваются просто формулируемые свойства, связанные с применением операции произведения (конкатенации) формальных языков – причём не обязательно (но обычно) языков конечных. Поэтому – если говорить с точки зрения алгебры полугрупп – исследуемыми задачами можно назвать некоторые просто формулируемые свойства глобальных надмоноидов свободных моноидов; из такого описания понятно, что основной рассматриваемой операцией является конкатенация.

Далее обычно будем говорить просто «глобальные надмоноиды»; при этом отметим, что термин «супермоноиды», по мнению автора, отечественными алгебраистами не одобряется – несмотря на то, что в английской литературе слово “supermonoid” употребляется часто. Отсюда – достаточно громоздкое название статьи [1]. Также по этому поводу заранее отметим, что рассматриваемые далеее проблемы равенства выполняются в глобальных надмоноидах не только свободных моноидов, но и более общих объектов – моноидов с левым законом сокращения. Однако для того, чтобы строго это доказать, или – иными словами – чтобы и для последних объектов были верными приведённые далее доказательства, необходимо было бы и для них строго определить понятия, соответствующие понятиям длины, префиксности и т. п., а также доказать некоторые свойства этих понятий; в настоящей статье такие задачи не ставятся.

Последние упомянутые объекты (глобальные надмоноиды) также являются моноидами, см. подробнее [2]. Иногда ниже будет допускаться случай, когда исходные свободные моноиды имеют бесконечное число образующих (атомов). То есть – по терминологии теории формальных языков – будут рассматриваться языки, заданные над произвольным алфавитом – возможно, бесконечным.

В глобальных надмоноидах рассматриваются некоторые специальные проблемы равенства (т. е. задачи формулирования необходимых и достаточных условий этих равенств). Среди подобных проблем – исследование равенства $A^m = B^n$. Доказывается, например, что в случае префиксных языков это равенство равносильно наличию у множеств A и B общего корня, определяемого для операции конкатенации обычным образом [1]. Заранее отметим по этому поводу, что на основе:

- доказанного в [1] утверждения о свободности *префиксного* подмоноида;
- а также материала, изложенного в [3, § 6.6],

необходимые и достаточные условия этого равенства, а также «префиксного» случая равенства $AB = BA$, становится очевидными. Однако, по мнению автора, и доказательства, приведённое в настоящей статье, также могут представить интерес – например, для практи-

[1] При этом, на основании результатов наших предыдущих публикаций, а также зложенного далее в настоящей статье, можно утверждать, что в подобном префиксном случае корень заранее заданной степени извлекается не более чем одним способом. Однако в общем случае подобный факт неверен.

Статья получена 5 марта 2023 г.

Борис Феликсович Мельников, Университет МГУ – ППИ в Шэньчжэне (bormel@smbu.edu.cn).

ческих задач, связанных с возможными приложениями алгебры полугрупп к алгоритмам теории формальных языков.

Конкретные обоснования сказанного в предыдущем абзаце таковы: в самых разных задачах могут оказаться полезными следующие два аспекта возможных доказательств существования общего корня для двух коммутирующих префиксных языков.

- Во-первых, «алгебраический» аспект: при рассмотрении утверждений, связанных с исследованием упомянутого выше равенства $A^m = B^n$ ([4], [5]), важно лишь *существование* общего корня – а не его конкретный вид.
- И наоборот (во-вторых) – «алгоритмический» аспект: при создании программных продуктов для возможной проверки равенства двух контекстно-свободных языков нужны *эффективные алгоритмы построения* общего корня. Именно для этого оказываются полезными доказательства, приведённые в настоящей статье, – поскольку они являются конструктивными.

К этому добавим, что критерии всех рассматриваемых равенств были использованы автором в различных задачах теории формальных языков – в первую очередь в [6], [7].

Отметим, что некоторая часть материала настоящей статьи уже была опубликована ранее – в [4], [5], а также впоследствии в [8], [9], [10], [11]. Однако ни статья [4], ни монография [5] в Интернете недоступны, а в последующих вышеупомянутых работах автора была опубликована только часть материала настоящей статьи.

Перечислим и некоторые другие причины для настоящей публикации (мотивацию).

- Здесь применена новая терминология. Подробнее о ней и о старой терминологии см. в [12], а кратко – ниже в разделе II.
- Во многих утверждениях изменены входные условия – причём обычно «в сторону бóльших возможностей» для рассматриваемых в этих условиях языков; о сделанных изменениях всегда будут приводиться замечания в тексте статьи.
- Всюду по тексту статьи будет отмечаться возможная связь формулируемых утверждений с инверсными морфизмами (в том числе с т. н. оптимальным инверсным морфизмом, см. [12], [13], [14], а также приведённые в этих работах другие ссылки); об этой связи в указанных выше публикациях почти не говорилось.
- В недавней публикации [15] мы рассматривали связанные вопросы. При этом, как мы надеемся, результаты настоящей статьи удастся применить для [15] – и наоборот, результаты статьи [15] удастся применить для некоторых задач, рассматриваемых в настоящей статье.
- Результаты настоящей статьи предполагается применить и в готовящейся статье про максимальные префиксные коды – также связанные с алгоритмами построения оптимального инверсного морфизма[2].

  При этом формулировки некоторых утверждений изменены так, чтобы их было удобно применять при исследовании множеств максимальных префиксных кодов. Автор предполагает, что такую статью можно будет рассматривать и как продолжение [8], [9].

[2] Причём связаны не только сами результаты, но и применённые для доказательства утверждений приёмы. В частности (но не только) мы в другой ситуации будем строить примерно ту же конструкцию, которая используется ниже при доказательстве утверждения 6.

Кратко опишем содержание статьи по разделам. *Раздел II* – предварительные свéдения, в нём приведены применяемые обозначения, в том числе нестандартные. *В разделе III* приведены несколько вспомогательных утверждений, связанных с возможным выбором левого делителя для заданного языка.

В разделе IV рассматриваются те из результатов предыдущего раздела III, которые удачно переформулируются, если рассматриваемые в утверждениях языки могут быть получены в результате действия морфизмов; при этом мы формулируем полученные результаты таким образом, чтобы их можно было применять и «в результате раскодирования», т. е. после действия инверсных морфизмов.

Краткое описание содержания *раздела V* полностью определяется его названием – «Об общем корне в глобальном надмоноиде». К этому стóит добавить, что материал раздела связан с вышеупомянутой статьёй [15].

Последующие разделы включены в часть II настоящей статьи.

Утверждения и теорема *раздела VI* описывают формулировки «выходных» ограничений – т. е. тех, которые можно вывести на основе специальных «входных» ограничений и (что является основным предметом раздела) условия коммутирования двух языков. В *разделе VII* к таким «входным» ограничениям мы добавляем условие префиксности рассматриваемых языков. *Раздел VIII* – случай 1- или 2-элементных языков; материалы этого раздела частично опубликованы в [10], [11].

Раздел IX – заключение; в нём приводятся различные интересные примеры, а также формулируются пока не решённые задачи.

II. ПРЕДВАРИТЕЛЬНЫЕ СВÉДЕНИЯ

В этом разделе приведены применяемые обозначения, в том числе нестандартные. Некоторые из обозначений ранее нами определялись в предыдущих статьях – но, по-видимому, без их повторения настоящая статья была бы существенно сложнее для понимания.

Однако начнём раздел с описания обозначений стандартных. Смысл слова «умножение» для рассматриваемых объектов понятен: это просто результат произведения (конкатенации) двух языков. В частности, рассмотрим такой пример для 1-буквенного алфавита: если

$$C = \left\{ a^i \,\middle|\, i \in I \right\} \quad \text{и} \quad D = \left\{ a^j \,\middle|\, j \in J \right\}$$

(I и J – некоторые конечные подмножества целых неотрицательных чисел), то

$$C \cdot D = \left\{ a^k \,\middle|\, (\exists\, i \in I,\, j \in J)\,(k = i + j) \right\}.$$

Легко доказывается, что эта операция ассоциативна (просто потому, что ассоциативной по определению является такая операция в свободном моноиде) – и поэтому можно говорить о рассмотрении глобального надмоноида (с единицей $\{\varepsilon\}$). Слово «умножение» будем в дальнейшем применять без кавычек. На основе произведения естественным образом определяется степень языка. Аналогично для «деления» [3] и слов, производных от «умножения» и «деления».

Для упрощения формулировок утверждений все рассматриваемые в этой главе языки (элементы глобального надмоноида), *обозначаемые заглавными латинскими буквами, предполагаются непустыми и, если не сказано иного, отличными от нуля* (нуля глобального надмоноида – пустого языка $\varnothing$).

Ещё немного про операцию конкатенации: аналогично другим публикациям, мы иногда употребляем само обозначение этой операции (обычно – если мы хотим подчеркнуть, как именно получено множество-произведение), а иногда его опускаем (наоборот – если способ получения произведения непринципиален). Понятно, что «чёткой границы» между этими двумя ситуациями не существует.

Для заданного слова $u \in \Sigma^*$:

- язык $\mathrm{pref}(u)$ определяется как множество префиксов слова u (включая несобственный, само u);
- язык $\mathrm{opref}(u)$ определяется как множество собственных префиксов слова u;
- язык $\mathrm{suff}(u)$ определяется как множество суффиксов слова u (включая несобственный, само u);
- язык $\mathrm{osuff}(u)$ определяется как множество собственных суффиксов слова u.

Для заданного языка $A \subseteq \Sigma^*$

$$\mathrm{pref}(A) = \bigcup_{u \in A} \mathrm{pref}(u)\,;$$

аналогичным образом определяются $\mathrm{opref}(A)$, $\mathrm{suff}(A)$ и $\mathrm{osuff}(A)$.

Если язык A обладает свойством префикса – т. е.

$$(\forall u, v \in A,\ u \neq v)\ (u \notin \mathrm{opref}(v)),$$

то будем писать $\mathrm{Pr}(A)$. Аналогично пишем $\mathrm{Su}(A)$ в случае, если язык A обладает свойством суффикса.

Морфизм (использование этого термина согласовано с [16]) – это отображение

$$h : \Delta^* \to \Sigma^*,$$

для которого:

- для каждой буквы $d \in \Delta$ её образ $h(d) \in \Sigma^*$ задаётся;
- а для каждого слова $d_1 d_2 \dots d_n \in \Delta^*$ полагаем

$$h(d_1 d_2 \dots d_n) = h(d_1)\, h(d_2) \dots h(d_n).$$

Конкретно, для некоторого языка

$$A \in \Sigma^*, \quad A = \{ u_1, u_2, \dots u_n \}$$

мы рассматриваем алфавит

$$\Delta_A = \{ d_1, d_2, \dots d_n \}$$

(если это не вызывает неоднозначностей, пишем обычно просто Δ), а для последнего – морфизм

$$h_A : \Delta_A^* \to \Sigma^*,$$

задающийся следующим образом:

$$h_A(d_1) = u_1\,,\ h_A(d_2) = u_2\,,\ \dots\,,\ h_A(d_n) = u_n\,.$$

Будем такой морфизм называть A-морфизмом [4]. Если при этом язык A не обладает свойством префикса, то определённый здесь морфизм также будем называть *непрефиксным*.

Для дальнейшего важной является следующая задача построения *инверсного* морфизма. Для заданных конечного языка A, морфизма h_A и некоторого слова $u \in \Sigma^*$ рассматриваем *язык* [5]

$$h_A^{-1}(u) = \{ u_\Delta \in \Delta^* \mid h_A(u_\Delta) = u \}\,;$$

специально отметим, что определяемое понятие является *множеством*.

Ту же самую конструкцию можно рассматривать и для некоторого языка (пусть B, вместо слова u) – причём нас будут интересовать только конечные языки:

$$h_A^{-1}(B) = \bigcup_{u \in B} h_A^{-1}(u).$$

$\|A\|_{\min}$ – длина минимального слова в языке A, $\|A\|_{\max}$ – длина максимального слова в этом языке.

Вместо бинарного отношения $\tilde{\infty}$, рассматривавшегося в [4], [5] и других работах 1990-х годов, мы начиная со статей, опубликованных в 2019 г., рассматриваем бинарные отношения $\between$ и $\trianglelefteq$; называем их «новыми обозначениями» – но фактически в новых статьях для этих обозначений проведена переформулировка большинства старых результатов.

Повторим определение бинарного отношения $\between$ и связанных с ним понятий. Если для конечных языков A и B выполнено условие

$$(\forall u \in A^*)\ (\exists v \in B^*)\ (u \in \mathrm{opref}(v)),$$

будем писать $A \trianglelefteq B$ (либо $B \trianglerighteq A$). Если одновременно выполнены условия $A \trianglelefteq B$ и $A \trianglerighteq B$, будем писать $A \between B$. Наоборот, в случае, когда уже известно, что условие $A \trianglerighteq B$ не выполнено, мы в случае выполнения условия $A \trianglelefteq B$ можем также писать $A \triangleleft B$ (либо $B \triangleright A$).

$\overline{1, n}$ – это множество $\{1, 2, \dots, n\}$ для рассматриваемого $n \in \mathbb{N}$.

Понятия, связанные с недетерминированными конечными автоматами, мы здесь повторять не будем: в настоящей статье они будут нужны только в одном утверждении, где мы и приведём небольшие подробности

III. ПОИСК ЛЕВОГО ДЕЛИТЕЛЯ: ВСПОМОГАТЕЛЬНЫЕ УТВЕРЖДЕНИЯ

В этом разделе приведены несколько вспомогательных утверждений, связанных с возможным выбором левого делителя для заданного языка. Доказательства первых трёх утверждений (1–3) не сложны, поэтому далее будем ими обычно пользоваться без специальных ссылок.

Утверждение 1: Если $\mathrm{Pr}(A)$ и $A \cdot B = A \cdot C$, то $B = C$. $\square$

[3] При этом отметим, что такая операция – при заданных «делимом» и «делителе» – вообще говоря, не является однозначной. Однако мы в настоящей статье либо доказываем однозначность (при некоторых заданных условиях), либо явно указываем на её невыполнение.

[4] Несмотря на то, что язык A рассматривается как множество – а *не* как упорядченное множество – неточностей в таких обозначениях нет.

[5] Состоящий, вообще говоря, не из одного, а из нескольких слов – а, возможно, являющийся пустым языком.

Это – просто левый закон сокращения в префиксном подмоноиде глобального надмоноида (т. е., иными словами, левый закон сокращения для языков, обладающих свойством префикса).

Утверждение 2: Если $\Pr(A)$ и $\Pr(B)$, то $\Pr(AB)$. □

Утверждение 3: Если $\Pr(AB)$, то $\Pr(B)$. □

Примеры конкретных языков, поясняющие утверждения 1–3, также несложны и в настоящей статье опущены.

Утверждение 4: Пусть

$$\Pr(A),\ \Pr(B) \quad \text{и} \quad AX = BY$$

для каких-либо языков X и B. Тогда

$$(\exists\, C)\ (A = BC \text{ или } B = AC)\,. \tag{1}$$

Замечание. Утверждение с именно такой формулировкой было ранее рассмотрено в двух работах – [4], [5]. Вместо префиксности B можно потребовать суффиксность Y, доказательство при этом немного изменится, см. подробнее [6]. Однако все указанные изменения незначительны, поэтому мы не будем приводить в настоящей статье оба варианта – но ниже будем употреблять ссылку на данное утверждение 4 для обеих указанных формулировок.

Доказательство. Если $A = B$, то сформулированное утверждение выполняется для $C = \{\varepsilon\}$. Поэтому будем далее полагать, что $A \neq B$.

Предположим, что $u \in A$, и при этом

$$uv \in B \tag{2}$$

для некоторых слов u и $v \neq e$ (случай $u \in B$, $uv \in A$ рассматривается аналогично). Тогда согласно $\Pr(A)$ и $AX = BY$ выполнено условие $vY \subseteq X$. Поэтому для произвольного $v' \in A$ имеем следующее:

$$(\forall y \in Y)\ (u'vy \in AX = BY)\,,$$

и, вследствие условия $\Pr(B)$, получаем $u'v \in B$.

Таким образом, для рассматриваемого v выполняется утверждение

$$(\forall u' \in A)\ (u'v \in B)\,.$$

Следовательно, для множества C, состоящего из всех слов v, которые могут быть выбраны согласно (2), выполнено равенство $AC = B$. □

Заметим ещё, что оба случая одновременно – т. е. и

$$(\exists\, u, v \neq e)\,(u \in A, uv \in B)\,,$$

и

$$(\exists\, u, v \neq e)\,(u \in B, uv \in A)\ -$$

не могут иметь места из-за $\Pr(A)$. (Согласно доказанному выше, эти условия эквивалентны равенствам $A = BC$ и $B = AC'$ соответственно, причём $C \neq \{\varepsilon\}$ и $C' \neq \{\varepsilon\}$.)

Утверждение 5: Пусть

$$\Pr(A),\ \Pr(L) \quad \text{и} \quad A^m L = L B^n$$

для некоторых $m, n \in \mathbb{N}$. Тогда

$$(\exists \widetilde{A})\ (AL = L\widetilde{A})\,,$$

причём $\Pr(\widetilde{A})$ и $\widetilde{A}^m = B^n$.

Замечание. В [6] при формулировке аналогичного утверждения было наложено дополнительное ограничение – суффиксность языка B. Аналогично и для дальнейших утверждений: в соответствующих им утверждениях статьи [6] были наложены более жёсткие ограничения, применимые, однако, для решаемых в [6] задач.

Доказательство. Если $A = \{\varepsilon\}$, то вследствие условия $L = LB^n$ выполнено $B = \{\varepsilon\}$, и доказываемое утверждение очевидно. Поэтому будем далее полагать, что $A \neq \{\varepsilon\}$.

Для доказательства построим следующим образом конечную последовательность языков L_i, где $i \in \overline{1, r}$ для некоторого натурального r. Пусть $i = 0$ и $L_0 = L$. По условию, выполнено $\Pr(L_i)$, и, кроме того,

$$A^m L_i = L_i B^n$$

для выбранного нами $i = 0$ и заданных m, n, A и B.

Теперь предположим, что для некоторого i выполнены условия

$$\Pr(L_i) \quad \text{и} \quad A^m L_i = L_i B^n\,.$$

Обозначив

$$X = A^{m-1} L_i \quad \text{и} \quad Y = B^n\,,$$

получаем, что согласно утверждению 4 для некоторого языка C выполнено или

$$A = L_i C, \tag{3}$$

или

$$L_i = AC. \tag{4}$$

Если выполняется первое условие – (3), то

$$(L_i C)^m L_i = L_i B^n\,, \quad \text{т. е.} \quad L_i (C L_i)^m = L_i B^n\,,$$

и обозначив $\widetilde{A} = CL_i$, получаем $\widetilde{A}^m = B^n$. Вследствие $\Pr(L_i)$ выполнено условие $\Pr(\widetilde{A})$ согласно (3).

Если же выполняется (4), то обозначив $L_{i+1} = C$, мы можем записать заданное условие в виде

$$A^m A L_{i+1} = A L_{i+1} B^n,$$

поэтому

$$A^m L_{i+1} = L_{i+1} B^n.$$

Таким образом, мы смогли построить нужныйнам язык L_{i+1} для нового индекса $i + 1$. Заметим, что

$$\|L_{i+1}\|_{\min} < \|L_i\|_{\min}$$

(т. к. $L_i = AL_{i+1}$ и $A \neq \{\varepsilon\}$), поэтому построенная последовательность множеств – конечная, и поэтому для некоторого натурального i выполнено условие (3).

Покажем, что $AL = L\widetilde{A}$. Пусть i – такое число, что выполнено условие (3). На основе метода построения L_i заключаем, что выполнено равенство $L = A^i L_i$. Из (3) и $\widetilde{A} = CL_i$ следует $AL_i = L_i\widetilde{A}$. Поэтому

$$A^{i+1} L_i = A^i L_i \widetilde{A}\,,$$

а из последнего получаем $AL = L\widetilde{A}$. □

Утверждение 6: Пусть $\Pr(A)$ и для некоторых B, X и Y выполнены равенства

$$AX = XB \quad \text{и} \quad AY = YB\,.$$

Пусть также

$$\|X\|_{\min} \leqslant \|Y\|_{\min}.$$

Тогда

$$(\exists Z)\,(Y = XZ).$$

Доказательство. Если $A = \{\varepsilon\}$ (что равносильно тому, что $B = \{\varepsilon\}$), то выполнение доказываемого условия очевидно. Поэтому будем далее предполагать, что $A \neq \{\varepsilon\}$ и $B \neq \{\varepsilon\}$.

Будем в этом доказательстве для произвольного языка Q использовать такое сокращение:

$$\|Q\| = \|Q\|_{\min}.$$

Построим конечную последовательность пар языков (X_i, Y_i), такую что при каждом i для X_i вместо X и Y_i вместо Y выполнены условия доказываемого утверждения. Базис этого рекуррентного процесса построения пар множеств следующий:

$$X_0 = X\,,\ \ Y_0 = Y\,.$$

Процесс финиширует, если

$$\|X_i\| < \|A\|\,. \tag{5}$$

Опишем шаг процесса.

По предположению индукции, $\|X_i\| \geqslant \|A\|$, поэтому согласно утверждению 4, $X_i = AC$ для некоторого C.

$$\|Y_i\| \geqslant \|X_i\|\ , \quad \text{отсюда} \quad \|Y_i\| \geqslant \|A\|\ ,$$

поэтому выполняется равенство

$$Y_i = AC'$$

для некоторого языка C'. Обозначив

$$X_{i+1} = C \quad \text{и} \quad Y_{i+1} = C'\,,$$

получаем, что согласно

$$AX_i = X_i B \quad \text{и} \quad AY_i = Y_i B\,,$$

выполнены условия

$$AAX_{i+1} = AX_{i+1}B \quad \text{и} \quad AAY_{i+1} = AY_{i+1}B\,,$$

т. е.

$$AX_{i+1} = X_{i+1}B \quad \text{и} \quad AY_{i+1} = Y_{i+1}B\,.$$

Таким образом, мы построили новую пару множеств. Заметим ещё, что

$$X = A^i X_i \quad \text{и} \quad Y = A^i Y_i$$

для произвольного i.

Описанный процесс не является бесконечным, т. к. согласно сделанному предположению $A \neq \{\varepsilon\}$, выполнены условия

$$\|X_{i+1}\| < \|X_i\| \quad \text{и} \quad \|Y_{i+1}\| < \|Y_i\|\ .$$

Таким образом, мы можем рассмотреть число i, для которого верно неравенство (5). Согласно утверждению 4, выполнено условие $A = X_i D$ для некоторого множества D. Возможны два варианта:

- $\|Y_i\| < \|A\|$, поэтому $A = Y_i D'$ для некоторого D', тогда
$$Y_i D' = X_i D\,,$$
и аналогично утверждению 4 доказываем, что
$$Y_i = X_i Z$$
для некоторого Z.
- $\|Y_i\| \geqslant \|A\|$, поэтому согласно утверждению 4,
$$Y_i = AD''$$
для некоторого D'', а из последнего получаем равенство
$$Y_i = X_i D D''\,.$$

Итак, в обоих случаях выполнено равенство $Y_i = X_i Z$ для некоторого языка Z (во втором случае $Z = DD''$). Поэтому

$$A^i Y_i = A^i X_i Z\,,$$

и, согласно ранее отмеченному, $Y = XZ$. □

IV. ДЕЛИТЕЛИ КАК РЕЗУЛЬТАТЫ ДЕЙСТВИЯ МОРФИЗМОВ И ИНВЕРСНЫХ МОРФИЗМОВ

В этом разделе рассматриваются те из результатов раздела предыдущего, которые удачно переформулируются, если рассматриваемые в утверждениях языки могут быть получены в результате действия морфизмов; при этом мы формулируем полученные результаты таким образом, чтобы их можно было применять и «в результате раскодирования», т. е. после действия инверсных морфизмов.

Отметим, что практически все рассматриваемые в статье задачи можно связать с развитием (обобщением) т. н. «задачи Пэна» [17] – т. е. с тем фактом, что инверсный морфизм регулярного языка регулярен.

Утверждение 7: Для любого регулярного языка B и любого морфизма h язык $h^{-1}(B)$ регулярен.

Замечание. Ранее автором настоящей статьи уже было опубликовано доказательство этого факта, более простое, чем доказательство самóго Пэна – см. [18]. Однако для более детального описания результатов настоящей статьи приведём краткий вариант этого доказательства ещё раз.

Доказательство. Пусть регулярный язык B задан. Рассмотрим произвольный определяющий его конечный автомат

$$K = (Q, \Sigma, \delta, S, F).$$

(Все обозначения, связанные с автоматами, согласованы с применяемыми в наших предыдущих публикациях – см. [19] и др.; при необходимости см. также [17].)

Далее рассмотрим автомат (с тем же самым множеством состояний, в том числе стартовых и финальных)

$$K_\Delta = (Q, \Delta, \delta_\Delta, S, F),$$

где функция δ_Δ определяется следующим образом:

$$\delta_\Delta(q, a) \ni q'$$

(для некоторых $q, q' \in Q$ и $a \in \Delta$) тогда и только тогда, когда язык автомата

$$K_{q,q'} = (Q, \Sigma, \delta, \{q\}, \{q'\})$$

содержит слово $h(a)$. (Заметим, что последний автомат, вообще говоря, не является детерминированным, т.к. $\delta_\Delta(q, a)$ определяется неоднозначно. В любом случае, мы привели корректное *конструктивное* определение функции δ_Δ.) Или, применяя другую систему обозначений: условие $\delta_\Delta(q,a) \ni q$' выполнено тогда и только тогда, когда

$$p \xrightarrow[K]{h(a)} r.$$

Очевидно, что автомат K_Δ определяет некоторое слово (над алфавитом Δ) тогда и только тогда, когда морфический образ этого слова определяется автоматом K (последний при принятии этого слова *может* оказаться в одном из состояний множества F) – и поэтому автомат K_Δ определяет язык $h^{-1}(B)$, что и требовалось доказать. □

Произведённое в утверждении 7 (в «задаче Пэна») изменение исходных условий можно рассматривать при применении к исходным языкам любого инверсного морфизма – причём для обеих задач, сформулированных в этом и следующем разделах, а также, возможно, и для некоторых других утверждений настоящей статьи.

Перейдём к рассмотрению основного утверждения раздела.

Утверждение 8: Пусть

$$AL = L\widetilde{A}\,, \quad B = h_A(C)$$

для некоторого $C \in mp(\Delta)$ и

$$BL = L\widetilde{B} \tag{6}$$

для некоторого $\widetilde{B}$. Тогда

$$\widetilde{B} = h_{\widetilde{A}}(C)\,.$$

Примеры к утверждению. Перед доказательством приведём две группы примеров, описывающих возможные языки C:

- L состоит ровно из одного слова, тогда C – произвольный язык из множества $mp(\Delta)$;
- $C = \Delta^n$ для некоторого $n \in \mathbb{N}$.

В обоих случаях, конечно, должны выполняться и остальные сформулированные условия.

Какие-либо другие примеры автору неизвестны. И, по-видимому, верно и более сильное утверждение, требующее, кроме равенства

$$\widetilde{B} = h_{\widetilde{A}}(C)\,,$$

ещё и выполнения одного из условий, рассмотренных в приведённых здесь примерах. Отметим ещё, что в статье [4] для доказываемых в этой работе теорем такого более сильного утверждения (если оно действительно верно) не понадобилось: равенство $C = \Delta^n$ там было получено на основе других соображений.

Доказательство. Будем в этом доказательстве использовать такое сокращение:

$$\|Q\| = \|Q\|_{\max}$$

для произвольного языка Q.

Докажем требуемый факт индукцией по $\|C\|$. Базис очевиден, т. к. существует единственный язык C из множества $mp(\Delta)$, для которого $\|C\| = 1$: это – $C = \Delta$, а из последнего получаем

$$B = A \quad \text{и} \quad \widetilde{B} = \widetilde{A}\,.$$

Далее будем доказывать шаг индукции.

Пусть

$$C = C_1 \cup C_2\Delta\,,$$

где

$$\|C_2\|_\forall = \|C\| - 1 \quad \text{и} \quad \|C_1\| < \|C\|\,.$$

Заметим, что

$$C' = C_1 \cup C_2 \in mp(\Delta)\,,$$

причём такое представление в виде объединения множеств C_1 и $C_2\Delta$ всегда единственно. Обозначим

$$B_1 = h_A(C_1)\,, \quad B_2 = h_A(C_2)\,, \quad B' = h_A(C')\,.$$

Тогда согласно заданному условию (6) имеем равенства

$$B_1L = L\widetilde{B}_1 \quad \text{для} \quad \widetilde{B}_1 = h_{\widetilde{A}}(C_1)\,,$$

а также

$$h_A(C_2\Delta)L = LX$$

для некоторого X.

Согласно последнему равенству,

$$h_A(C_2)L = L\widetilde{B}_2 \quad \text{для} \quad \widetilde{B}_2 = h_{\widetilde{A}}(C_2)\,,$$

т. е. $B_2L = L\widetilde{B}_2$. Поэтому

$$B' = h_A(C') = h_A(C_1 \cup C_2) =$$

$$= h_A(C_1) \cup h_A(C_2) = L\widetilde{B}_1 \cup L\widetilde{B}_2 = L\widetilde{B}'$$

для некоторого $\widetilde{B}'$.

Согласно предположению индукции,

$$\widetilde{B}' = h_{\widetilde{A}}(C')\,.$$

Отсюда получаем

$$Lh_{\widetilde{A}}(C) = Lh_{\widetilde{A}}(C_1) \cup Lh_{\widetilde{A}}(C_2\Delta) =$$

$$= L\widetilde{B}_1 \cup Lh_{\widetilde{A}}(C_2)h_{\widetilde{A}}(\Delta) = L\widetilde{B}_1 \cup L\widetilde{B}_2\widetilde{A} =$$

$$= B_1L \cup B_2AL = (B_1 \cup B_2A)L = BL.$$

Таким образом,

$$Lh_{\widetilde{A}}(C) = BL\,,$$

и вследствие (6) выполнено равенство

$$\widetilde{B} = h_{\widetilde{A}}(C)\,,$$

доказывающее шаг индукции. □

V. ОБ ОБЩЕМ КОРНЕ В ГЛОБАЛЬНОМ НАДМОНОИДЕ

Краткое описание содержания этого раздела полностью определяется его названием. Добавим лишь, что материал раздела связан с нашей недавно опубликованной статьёй [15].

Утверждение 9: Пусть $Pr(A)$ и для некоторых $m, n \in \mathbb{N}_0$ выполнено равенство

$$A^m = B^n. \tag{7}$$

Тогда

$$(\exists C, m', n')\,(A = C^{n'}, B = C^{m'})\,.$$

Доказательство. Без ограничения общности можно предполагать, что $m \leqslant n$. Тогда согласно утверждению 4, $A = BQ$ для некоторого языка Q (мы допускаем возможность $Q = \{\varepsilon\}$). Выберем максимальное число p_1, для которого

$$(\exists Q)\ (A = B^{p_1} Q)\,.$$

Обозначим $A_1 = Q$ (этот язык однозначно определяется согласно представлению A в виде $A = B^{p_1} A_1$); тогда мы можем записать (7) таким образом:

$$(B^{p_1} A_1)^m = B^n. \tag{8}$$

Из последнего получаем:

$$A_1 (B^{p_1} A_1)^{m-1} = B^{n-p_1} \tag{9}$$

(при этом очевидно, что $n \geqslant p_1$).

Согласно (9) и утверждению 4, имеем $B = A_1 Q$ для некоторого языка Q (т. к. равенство $A_1 = B^{p_1} Q$ для произвольного $Q \neq \{\varepsilon\}$ невозможно из-за способа выбора p_1). Выберем аналогично число q_1 и введём множество B_1 согласно равенству $B = A_1^{q_1} B_1$ (число q_1 – также максимально возможное). На основе введённых обозначений мы можем записать (7) таким образом:

$$((A_1^{q_1} B_1)^{p_1} A_1)^m = (A_1^{q_1} B_1)^n. \tag{10}$$

Продолжая этот процесс аналогично проделанному в доказательствах утверждений 5 и 6, определяем конечные последовательности пар множеств A_i и B_i. При этом числа p_i, q_i и языки A_i, B_i определяются из условий

$$A_{i-1} = B_{i-1}^{p_i} A_i \quad \text{и} \quad B_{i-1} = A_{i-1}^{q_i} B_i\,.$$

Таким образом, после этих переобозначений мы можем переписать исходное равенство (7) следующими способами:

$$((\ldots(((B_{i-1})^{p_{i-1}} A_i)^{q_{i-1}} B_{i-1})^{p_{i-2}} \ldots B_{i-1})^{p_1} A_i)^m =$$
$$= (\ldots(((B_{i-1})^{p_{i-1}} A_i)^{q_{i-1}} B_{i-1})^{p_{i-2}} \ldots B_{i-1})^n \tag{11}$$

и

$$((\ldots(((A_i)^{q_{i-1}} B_i)^{p_{i-1}} A_i)^{q_{i-2}} \ldots B_i)^{p_1} A_i)^m =$$
$$= (\ldots(((A_i)^{q_{i-1}} B_i)^{p_{i-1}} A_i)^{q_{i-2}} \ldots B_i)^n \tag{12}$$

соответственно. Заметим, что равенства (11) и (12) выполняются и на первом шаге (т. е. для языков A_1 и B_1) – если считать

$$A_0 = A \quad \text{и} \quad B_0 = B\,;$$

эти равенства на первом шаге суть условия (8) и (10). Возможность выбора p_{i-1} и A_i для каждого следующего i – это следствие (12), а возможность выбора q_i и B_i – следствие (11).

Описанный процесс конечен, т. к. для произвольного рассматриваемого i выполнены условия

$$\|A_i\|_{\min} < \|A_{i-1}\|_{\min} \quad \text{и} \quad \|B_i\|_{\min} < \|B_{i-1}\|_{\min}\,.$$

Поэтому для некоторого $r \in \mathbb{N}$ либо $p_r = 0$, либо $q_r = 0$.

Пусть $p_r = 0$ (случай $q_r = 0$ рассматривается аналогично). Тогда $A_r = B_r$ (поскольку неравенство $A_r \neq B_r$ противоречит тому, что число q_{r-1} в (12) – максимально возможное). Обозначив

$$C = A_r = B_r\,,$$

мы легко доказываем равенства

$$A = C^{n'} \quad \text{и} \quad B = C^{m'}$$

для некоторых $n', m' \in \mathbb{N}$ индукцией по i для

$$i = r,\ r-1,\ \ldots,\ 1,\ 0\,,$$

используя при этом (11) и (12). □

Замечание. Если в доказанном утверждении обозначить через k наибольший общий делитель чисел m и n, то очевидно, что

$$n' = n/k \quad \text{и} \quad m' = m/k\,.$$

Вообще, можно провести аналогию между утверждением 9 с одной стороны – и, с другой стороны, легко доказываемым фактом из области арифметики, тоже формулирующимся с помощью (7), где, в отличие от доказанного утверждения, A, B и C – некоторые натуральные числа, причём C является общим корнем из чисел A и B (корнем разных степеней).

Как уже было отмечено, в части II настоящей статьи мы продолжим исследовать связь рассматриваемых в различных наших публикациях бинарных отношений, заданых на множестве конечных языков, – с условиями коммутирования таких языков.

VI. БЛАГОДАРНОСТИ

Работа частично поддержана грантом научной программы китайских университетов "Higher Education Stability Support Program" (раздел "Shenzhen 2022 – Science, Technology and Innovation Commission of Shenzhen Municipality").

Список литературы

[1] Мельников Б. *Описание специальных подмоноидов глобального надмоноида свободного моноида* // Известия высших учебных заведений. Математика. – 2004. – № 3. – С. 46–56.

[2] Скорняков Л. (ред.) *Общая алгебра. Том 2*. – М., Наука. – 1991. – 480 с.

[3] Кон П. *Свободные кольца и их связи*. – М., Мир. – 1975. – 422 с.

[4] Melnikov B. *Some equivalence problems for free monoids and for subclasses of the CF-grammars class* // Number theoretic and algebraic methods in computer science, World Sci. Publ. – 1995. – P. 125–137.

[5] Мельников Б. *Подклассы класса контекстно-свободных языков (монография)*. – М., Изд-во Московского университета. – 1995. – 174 с. – ISBN 5-211-03448-1.

[6] Дубасова О., Мельников Б. *Об одном расширении класса контекстно-свободных языков* // Программирование (РАН). – 1995. – № 6. – С. 46–58.

[7] Melnikov B., Kashlakova E. *Some grammatical structures of programming languages as simple bracketed languages* // Informatica (Lithuanian Academy of Sciences). – 2000. – Vol. 11. No. 4. – P. 441–454.

[8] Корабельщикова С., Мельников Б. *Максимальные префиксные коды и подклассы класса контекстно-свободных языков* // Вестник Северного (Арктического) федерального университета Серия: Естественные науки. – 2015. – № 1. – С. 121–129.

[9] Корабельщикова С., Мельников Б. *Итерации языков и максимальные префиксные коды* // Вестник Воронежского государственного университета. Серия: Физика. Математика. – 2015. – № 2. – С. 106–120.

[10] Корабельщикова С., Мельников Б. *Об общем корне элементов глобального надмоноида* // Вестник Северного (Арктического) федерального университета Серия: Естественные науки. – 2016. – № 3. – С. 91–96.

[11] Melnikov B., Korabelshchikova S., Dolgov V. *On the task of extracting the root from the language* // International Journal of Open Information Technologies. – 2019. – Vol. 7. No. 3. – P. 1–6.

[12] Мельников Б. *Полурешётки подмножеств потенциальных корней в задачах теории формальных языков. Часть III. Условие существования решётки* // International Journal of Open Information Technologies. – 2022. – Vol. 10. No. 7. – P. 1–9.

[13] Мельников Б. *Полурешётки подмножеств потенциальных корней в задачах теории формальных языков. Часть I. Извлечение корня из языка* // International Journal of Open Information Technologies. – 2022. – Vol. 10. No. 4. – P. 1–9.
[14] Мельников Б. *Полурешётки подмножеств потенциальных корней в задачах теории формальных языков. Часть II. Построение инверсного морфизма* // International Journal of Open Information Technologies. – 2022. – Vol. 10. No. 5. – P. 1–8.
[15] Мельников Б., Мельникова А. *О задачах извлечения корня из заданного конечного языка* // International Journal of Open Information Technologies. – 2023. – Vol. 11. No. 5. – P. 1–14.
[16] Саломаа А. *Жемчужины теории формальных языков*. – М., Мир. – 1986. – 159 с.
[17] Pin J.-E. *Mathematical Foundations of Automata Theory*. – Berlin, Springer-Verlag. – 2012. – 310 p.
[18] Мельников Б., Вылиток А., Мельникова Е. *Итерации языков и конечные автоматы* // International Journal of Open Information Technologies. – 2017. – Vol. 5. No. 12. – P. 1–7.
[19] Мельников Б. *Регулярные языки и недетерминированные конечные автоматы (монография)*. – М., Изд-во Российского государственного социального университета. – 2018. – 179 с. – ISBN 978-5-7139-1355-7.

Борис Феликсович МЕЛЬНИКОВ,
профессор Университета МГУ – ППИ в Шэньчжэне (`http://szmsubit.ru/`),
email$_1$: `bormel@smbu.edu.cn`,
email$_2$: `bf-melnikov@yandex.ru`,
mathnet.ru: `personid=27967`,
elibrary.ru: `authorid=15715`,
scopus.com: `authorId=55954040300`,
ORCID: `orcidID=0000-0002-6765-6800`.

On the connection of special binary relations with conditions of commuting languages. Part I. Divisors in the global supermonoid

Boris Melnikov

***Abstract*—The paper discusses various statements describing the connection of special binary relations (exactly, the binary relations of coverage and equivalence in infinity studied in our previous works) with the conditions of commuting languages. Generalizing, we are considering simply formulated properties associated with the use of the product operation (concatenation) of formal languages, not necessarily (but usually) finite languages. Among these problems, is the study of the conditions of equality of degrees of two languages. It is proved, for example, that in the case of prefix languages, such equality is equivalent to the presence of a common root of the considered sets, defined for the concatenation operation in the usual way.**

At the beginning of the paper, some auxiliary statements are given; they are related to the possible choice of its left divisor for a given language. Further, the obtained results about the left divisor are considered in particular, which are successfully reformulated if the languages considered in the statements can be obtained as a result of the action of any morphisms. Next, we consider the conditions for the presence of a common root in the global supermonoid for some its two elements.

After that, we consider various consequences of the condition of possible commutation of two languages: first in the general case, and then in the presence of the prefix condition of the given languages. At the end of the paper, some interesting examples are given, as well as the problems are formulated that have not yet been solved.

***Keywords*—formal languages, free monoid, supermonoids, iterations of languages, commutation, algorithms.**

References

[1] Melnikov B. *Description of special submonoids of the global supermonoid of the free monoid* // News of higher educational institutions. Mathematics. – 2004. – No. 3. – P. 46–56 (in Russian).

[2] Skornyakov L. (Ed.) *General Algebra. Vol. 2*. – Moscow, Nauka. – 1991. – 480 p. (in Russian).

[3] Cohn P. *Free rings and their relations*. – NY, Academic Press. – 1971. – 334 p.

[4] Melnikov B. *Some equivalence problems for free monoids and for subclasses of the CF-grammars class* // Number theoretic and algebraic methods in computer science, World Sci. Publ. – 1995. – P. 125–137.

[5] Melnikov B. *Subclasses of the context-free languages class (monograph)*. – Moscow, Moscow State University Ed. – 1995. – 174 p. – ISBN 5-211-03448-1 (in Russian).

[6] Dubasova O., Melnikov B. *On an extension of the class of context-free languages* // Programming and Computer Software (Russian Academy of Sciences Ed.). – 1995. – No. 6. – P. 46–54 (in Russian).

[7] Melnikov B., Kashlakova E. *Some grammatical structures of programming languages as simple bracketed languages* // Informatica (Lithuanian Academy of Sciences). – 2000. – Vol. 11. No. 4. – P. 441–454.

[8] Korabelshchikova S., Melnikov B. *Maximum prefix codes and subclasses of the context-free languages class* // Bulletin of the Northern (Arctic) Federal University. Series: Natural Sciences. – 2015. – No. 1. – P. 121–129 (in Russian).

[9] Korabelshchikova S., Melnikov B. *Iterations of languages and maximum prefix codes* // Bulletin of the Voronezh State University. Series: Physics. Math. – 2015. – No. 2. – P. 106–120 (in Russian).

[10] Korabelshchikova S., Melnikov B. *On the common root of elements of the global supermonoid* // Bulletin of Northern (Arctic) Federal University. Series: Natural Sciences. 2016. – No. 3. – P. 91–96. (in Russian)

[11] Melnikov B., Korabelshchikova S., Dolgov V. *On the task of extracting the root from the language* // International Journal of Open Information Technologies. – 2019. – Vol. 7. No. 3. – P. 1–6.

[12] Melnikov B. *Semi-lattices of the subsets of potential roots in the problems of the formal languages theory. Part III. The condition for the existence of a lattice* // International Journal of Open Information Technologies. – 2022. – Vol. 10. No. 7. – P. 1–9 (in Russian).

[13] Melnikov B. *Semi-lattices of the subsets of potential roots in the problems of the formal languages theory. Part I. Extracting the root from the language* // International Journal of Open Information Technologies. – 2022. – Vol. 10. No. 4. – P. 1–9 (in Russian).

[14] Melnikov B. *Semi-lattices of the subsets of potential roots in the problems of the formal languages theory. Part II. Constructing an inverse morphism* // International Journal of Open Information Technologies. – 2022. – Vol. 10. No. 5. – P. 1–8 (in Russian).

[15] Melnikov B., Melnikova A. *On the problems of extracting the root from a given finite language* // International Journal of Open Information Technologies. – 2023. – Vol. 11. No. 5. – P. 1–14 (in Russian).

[16] Salomaa A. *Jewels of Formal Language Theory*. – Rockville, Maryland, Computer Science Press. – 1981. – 144 p.

[17] Pin J.-E. *Mathematical Foundations of Automata Theory*. – Berlin, Springer-Verlag. – 2012. – 310 p.

[18] Melnikov B., Vylitok A., Melnikova E. *Iterations of languages and finite automata* // International Journal of Open Information Technologies. – 2017. – Vol. 5. No. 12. – P. 1–7 (in Russian).

[19] Melnikov B. *Regular languages and nondeterministic finite automata (monograph)*. – Moscow, Russian Social State University Ed. – 2018. – 179 p. – ISBN 978-5-7139-1355-7 (in Russian).

Boris MELNIKOV,
Professor of Shenzhen MSU – BIT University, China (`http://szmsubit.ru/`),
email$_1$: `bormel@smbu.edu.cn`,
email$_2$: `bf-melnikov@yandex.ru`,
mathnet.ru: `personid=27967`,
elibrary.ru: `authorid=15715`,
scopus.com: `authorId=55954040300`,
ORCID: `orcidID=0000-0002-6765-6800`.