**Белоусов А.И.**

УДК 519.76+372.851

# О некоторых свойствах полуколец

Россия, МГТУ им. Н.Э. Баумана

al\_belous@bk.ru

## Введение

Теория полуколец является важнейшей алгебраической основой для решения задач в теории графов, теории автоматов и формальных языков.

За последние несколько лет в теории полуколец получено немало интересных результатов, часть из которых касается собственно абстрактной алгебры [1 - 5], причем следует обратить особое внимание на работы, посвященные матрицам над полукольцами [6], а также исследованию неидемпотентных полуколец [2]. Большое значение имеют фундаментальные обзоры по итогам работ в этой области [1, 7, 8].

Приложениям теории полуколец к теории графов, автоматов и языков посвящен цикл работ авторов из Балтийского федерального университета им. И. Канта с участием известного специалиста в этой области В. Куиха (W. Kuich) – например, [9, 10]. В этой связи несомненный интерес представляет работа Н. С. Никулиной [11], в которой получены нетривиальные результаты по применению теории полуколец к решению задачи перечисления простых путей в графе. Эта работа по тематике близка к теме настоящей статьи, тем более, что автор ссылается на книгу [12], от некоторых идей которой и отправляется предлагаемая статья. В аспекте упомянутых приложений как раз наиболее важна структура идемпотентного полукольца. Исследованию свойств идемпотентных алгебр посвящены работы [13, 14]. Приложениям теории полуколец в криптографии посвящена работа [15].

Одно из важнейших приложений теории полуколец – теория автоматов. В этой связи заслуживает внимания статья [16], в которой рассматриваются приложения алгебраического аппарата полуколец к теории динамических систем.

В то же время остаются на повестке дня определенные методические проблемы, и теория полуколец является если не методической целиной, то областью, где необходимо тщательно проработать последовательность изложения теории в курсах алгебры или дискретной математики, пересмотреть доказательства некоторых теорем с целью их максимального упрощения, но без ущерба для строгости. По ходу решения методических проблем возникают и проблемы собственно научные, как правило связанные именно с поиском новых доказательств уже известных результатов.

С точки зрения методики и методологии большой интерес представляет статья Е. М. Вечтомова [17].

Данная статья носит научно-методический характер и в ней рассматриваются следующие вопросы.

Доказываются свойства бесконечной суммы (точной верхней грани последовательности по естественному порядку идемпотентного полукольца). Эти свойства подробно и в общем виде доказаны в [12], но излагаемые там доказательства весьма сложны, и в практике проведения занятий для студентов программистских специальностей целесообразно упростить некоторые доказательства. Важные свойства бесконечной суммы, из которых вытекает, в частности, непрерывность операции сложения, могут быть доказаны значительно проще. При этом приходится несколько жертвовать общностью анализа, но предлагаемый уровень вполне достаточен для нематематических специальностей бакалавриата.

Далее рассматриваются так называемые полукольца с итерацией и доказывается теорема о замкнутости таких полуколец относительно решений систем линейных уравнений. К полукольцам с итерацией относится и важнейшее для приложений к теории автоматов и языков полукольцо регулярных языков в заданном конечном алфавите.

После этого мы переходим к подробному изложению применения теории полуколец к решению общей задачи о путях в размеченных ориентированных графах. Здесь мы также следуем книге [12], но в отличие от нее во всех деталях доказываем основную теорему, согласно которой матрица стоимостей есть итерация матрицы меток дуг.

В целях полноты изложения кратко излагается (на основе [12]) метод вычисления матрицы стоимостей путем последовательного вычисления матриц стоимостей по путям различных (возрастающих) рангов. Это важно для доказательства основного результата статьи.

Также вводится специфическое для данной статьи понятие автомата над полукольцом (см. также [18]), который, в отличие от обычного размеченного орграфа имеет выделенную «заключительную» вершину с нулевой полустепенью исхода.

И в заключение доказывается основная теорема о том, что метод последовательного исключения неизвестных при решении системы линейных уравнений в полукольце с итерацией дает действительно наименьшее решение системы. Это доказательство основано на графовой интерпретации системы линейных уравнений. Подробное доказательство этой теоремы отсутствует в [12] и, приведенное здесь, восполняет существенный пробел. Особо следует подчеркнуть, что в процессе доказательства устанавливается связь между этим методом («методом Гаусса» для полуколец) и методом вычисления матрицы стоимостей для размеченного орграфа путем последовательного вычисления матриц стоимостей по путям возрастающих рангов. Оказывается, что эти два метода являются разными модификациями одного и того же алгоритма.

## Свойства бесконечной суммы

Под бесконечной суммой элементов  замкнутого полукольца [12] понимается точная верхняя грань последовательности , то есть, по определению

.

Точная верхняя грань рассматривается по естественному порядку идемпотентного полукольца, согласно которому , если .

Нижний предел суммирования может быть и больше нуля. Как правило, будем пользоваться обозначением , полагая по умолчанию, что суммирование ведется от нуля до бесконечности. В случае, когда нижний предел отличен от нуля, будем это указывать.

Рассмотрим здесь важнейшие свойства бесконечной суммы.

**Теорема 1**. Для произвольных последовательностей  и  имеет место равенство

.

**Доказательство**. Пусть . Докажем, что элемент  есть точная верхняя грань последовательности . Имеем: для любого  вычислим .

Если  - верхняя грань указанной последовательности, то , так как для любого  (конечная сумма есть, как известно, точная верхняя грань множества слагаемых [12]), т.е. элементявляется верхней гранью каждой из рассматриваемых двух последовательностей. Итак, , и .

Из доказанной теоремы вытекает важное свойство непрерывности операции сложения в замкнутом полукольце, а именно имеет место

**Следствие 1**. Для любых последовательности  и элемента замкнутого полукольца выполняется

.

**Доказательство**. Частный случай утверждения теоремы 1, когда вторая последовательность постоянна, то есть при  для каждого .

Итак, за бесконечную сумму можно выносить произвольное слагаемое, как и наоборот: вносить отдельное слагаемое в бесконечную сумму. Это и выражает свойство непрерывности операции сложения. Напомним, что операция умножения в замкнутом полукольце непрерывна по определению, то есть для последовательности  и элемента замкнутого полукольца выполняется

 и .

Это не что иное, как бесконечный аналог свойства дистрибутивности умножения относительно сложения.

Следующее свойство бесконечной суммы связано с понятием частичной суммы последовательности.

Положим для последовательности 

 при  и назовем это *k*-*ой частичной суммой* *последовательности* . Так как последовательность  является неубывающей, то  для любого .

**Теорема 2**. Точная верхняя грань (бесконечная сумма) любой последовательности равна точной верхней грани последовательности ее частичных сумм, то есть

.

**Доказательство**. Для произвольного неотрицательногоимеем:



(Использованы свойства коммутативности и идемпотентности операции сложения в полукольце.)

Это значит, что точная верхняя грань последовательности частичных сумм есть верхняя грань последовательности . Для произвольной верхней грани этой  последовательности аналогично предыдущему (доказательство теоремы 1), с учетом того, что для любого   получим: ,

откуда и следует доказываемое.

Доказанные выше свойства бесконечной суммы используются при доказательстве теоремы о наименьшем решении линейного уравнения



или

,

которое определяется формулой *x=ba\**, где *a*\* = - итерация (или замыкание элемента , для первого и *x=ba\** для второго уравнения в произвольном замкнутом полукольце (см. [12]).

## Полукольца с итерацией

*Полукольцо с итерацией* – это подполукольцо некоторого замкнутого полукольца, содержащее вместе с каждым своим элементом его итерацию.

Таким будет, например, полукольцо регулярных языков в произвольном конечном алфавите [12], которое, как известно, не является замкнутым, так как не любая бесконечная последовательность регулярных языков имеет регулярную точную верхнюю грань. Достаточно заметить, что язык , не будучи регулярным [19], может быть представлен как точная верхняя грань (в данном случае бесконечное объединение) последовательности регулярных языков (каждый член последовательности содержит одно слово  при произвольно фиксированном .

Мы докажем здесь, что компоненты решения системы линейных уравнений

 (1)

все коэффициенты которой принадлежат произвольному полукольцу с итерацией, принадлежат этому же полукольцу.

**Теорема 3**. Решение системы (1) есть вектор, компоненты которого принадлежат тому же полукольцу с итерацией, что и коэффициенты системы.

**Доказательство**. Индукция по порядку  системы (1).

При  система становится уравнением вида

.

Решение (в данном случае наименьшее) этого уравнения, как было указано выше, выражается формулой *x = a\*b*, а так как итерация любого элемента полукольца с итерацией принадлежит этому же полукольцу, то решение также будет элементом этого полукольца.

Базис доказан.

Формулируя стандартно индукционное предположение, рассмотрим систему (1) порядка . Выражая неизвестное  через остальные согласно формуле

 (2)

получим систему

 (3)

при , порядок которой равен , а все ее коэффициенты принадлежат рассматриваемому полукольцу с итерацией. В силу индукционного предположения вектор решения этой системы состоит из компонент, принадлежащих рассматриваемому полукольцу с итерацией. Согласно формуле (2) тогда и компонента  решения будет принадлежать этому же полукольцу.

Теорема доказана.

Можно также доказать, что метод последовательного исключения неизвестных при поиске решения системы (1), первый шаг которого описан в доказательстве теоремы 3, дает действительно наименьшее решение системы. Это будет доказано ниже. Здесь же мы доказали только замкнутость полукольца с итерацией относительно решений систем вида (1), получаемых согласно формулам (2) и (3).

Заметим, что само существование решения системы (1) доказано в [12].

## Размеченные орграфы и автоматы над полукольцами

Пусть  - орграф, на множестве дуг которого (множестве ) определена функция разметки *φ: E → S\*{0}, где  - носитель какого-то полукольца . Тогда орграф будем называть ***орграфом, размеченным над полукольцом***. Будем пока считать полукольцо  замкнутым (потом это требование будет ослаблено: мы увидим, что достаточно потребовать, чтобы это полукольцо было полукольцом с итерацией). Принимается также, что значение функции разметки на любой дуге графа не равно нулю полукольца.

Заметим, что ссылка на графы в статье нужна лишь для получения определенных алгебраических результатов. Поэтому мы не прибегаем здесь к каким-то иллюстрациям, так как собственно графический аспект тут не является существенным.

Орграф , размеченный над полукольцом , может быть задан квадратной матрицей -ого (где ) порядка , где . Эта матрица называется ***матрицей меток*** ***дуг размеченного орграфа***. Если полукольцо  есть двухэлементное полукольцо , то матрица весов дуг есть не что иное, как матрица смежности вершин.

Определим понятие ***метки пути в размеченном орграфе***. Пусть  - путь конечной длины . Дугу  этого пути обозначим через . Тогда если (т.е. есть путь нулевой длины), то метка *φ\*(W)* этого пути равна, по определению, единице полукольца. Иначе,

*φ\*(W) = φ(e*1*) φ(e*2*)… φ(em)*, т.е. *метка пути ненулевой длины определяется как произведение меток входящих в этот путь дуг (в порядке их прохождения)*.

***Стоимость прохождения из вершины в вершину*** , обозначаемая (или просто ) есть, по определению, сумма меток всех путей (конечной длины), ведущих из вершины в вершину . Если множество всех путей из в  конечно, то стоимость есть сумма в обычном смысле слова - *сумма элементов полукольца* . Если указанное множество бесконечно (но, так как рассматриваются только пути конечной длины, счетно - как бесконечное множество конечных последовательностей), то стоимость (для *замкнутого* полукольца ) есть *точная верхняя грань* множества меток всех путей из в . Если вершина  недостижима из вершины , то  по определению.

Итак, в любом случае мы можем написать:

 (4)

(принимая по определению, что в случае недостижимости вершины  недостижима из вершины записанная выше сумма, вообще говоря, бесконечная, равна нулю полукольца).

Определим теперь полукольцо матриц, чтобы корректно описать вычисление матрицы стоимостей.

Для любого (не обязательно замкнутого) полукольца  может быть определена алгебра  квадратных матриц -го порядка, где операции над матрицами производятся, как в обычной матричной алгебре, но с учетом того, что сложение и умножение элементов понимается в смысле того полукольца, которому принадлежат эти элементы.

Тогда может быть доказана теорема:

**Теорема 4**. Алгебра  есть полукольцо, причем, если полукольцо  замкнуто, то полукольцо матриц также замкнуто.

Доказательство приведено в [12].

Помимо матрицы стоимостей прохождения по всем путям в графе, может быть определена ограниченная матрица стоимостей прохождения по определенному множеству путей, например, по множеству путей заданной длины.

В общем случае можно определить для некоторого множества путей **P** стоимость прохождения из -й вершины в -ю по всем путям, принадлежащим множеству **P**, полагая в формуле (4), что суммирование идет только по путям из множества **P**.

Понятие ограниченной матрицы стоимостей будет использовано ниже.

**Теорема 5**. Матрица стоимостей  размеченного орграфа равна итерации (замыканию) матрицы  весов дуг:



**Доказательство**. Используя метод математической индукции, можно показать, что -ая степень матрицы меток дуг, т.е. матрица  есть матрица стоимостей по всем путям длины ().

Базис индукции ( ) тривиален: матрица стоимостей по всем путям длины 0 есть, очевидно, единичная матрица: . Пусть доказываемое справедливо для всех . Обозначая произвольный элемент матрицы  через , получим

.

Каждое слагаемое этой суммы есть произведение стоимости прохождения из вершины  в вершину  по всем путям длины  (это, по предположению индукции, элемент ) на элемент  матрицы смежности вершин, который при условии будет равен метке указанной дуги, а если такой дуги нет, то нулю полукольца. Это значит, что -ое слагаемое написанной выше суммы (для фиксированного ) будет либо равно нулю, либо будет суммой меток всех путей длины  из вершины  в вершину , последней дугой которого будет дуга .

Так как  пробегает все вершины графа, то сумма, выражающая элемент  будет ни чем иным, как суммой меток всех путей длины  из вершины  в вершину , т.е. стоимостью прохождения из вершины  в вершину  по всем путям длины .

Итак, сумма всех степеней матрицы  меток дуг размеченного орграфа будет матрицей стоимостей.

В некоторых работах [18] понятия размеченного над полукольцом орграфа и автомата над полукольцом отождествляются. Здесь же мы считаем целесообразным эти понятия несколько развести. А именно, автоматом над полукольцом  мы будем называть орграф, размеченный над этим полукольцом, в котором выделена вершина , называемая заключительной и имеющая нулевую полустепень исхода. Под языком такого автомата над полукольцом будем понимать сумму компонент вектора стоимостей прохождения из вершин графа, отличных от , в вершину . Заметим, что такой автомат понимается как обобщение понятия конечного автомата [12], так как в статье [18] рассматривается и обобщение понятия магазинного автомата для произвольного замкнутого полукольца. Тогда, если ввести вектор-столбец , в котором компонента  есть метка дуги, ведущей из *k*-ой вершины графа в вершину , если таковая есть, и нулю полукольца в противном случае, то указанный вектор стоимостей будет как раз равен *A\*b = Cb*, то есть будет наименьшим решением системы (1).

## Метод последовательного исключения неизвестных

В [12] подробно описан метод вычисления матрицы стоимостей с помощью последовательного вычисления матриц стоимостей по путям различных рангов.

Именно, ранг пути, ведущего из -й вершины в -ю, есть по определению наибольший номер вершины, лежащей на этом пути, не считая первой и последней (предполагается заранее заданной определенная нумерация вершин графа).

Принимается, что путь длины ноль, как и путь длины 1 (содержащий только одну дугу), имеет ранг, равный нулю.

Тогда элемент матрицы стоимостей прохождения по путям ранга, не большего , может быть записан в виде

,

где под знаком итерации находится стоимость прохождения по всем замкнутым путям, ранга, не большего , проходящим через -ю вершину (заметим, что в этих путях не допускается, следовательно, -я вершина как промежуточная).

Записанная выше формула означает, что идти по пути ранга, не большего , из -й вершины в -ю, можно либо «напрямую», минуя -ю вершину (первое слагаемое), либо пройти сначала из -й вершины в -ю (исключая эту последнюю как промежуточную), потом «покрутиться» по упомянутым выше замкнутым путям сколько угодно раз, а может быть, и ни разу, после чего проследовать в -ю вершину, опять-таки не «задевая» по пути -ю.

При этом исходная матрица стоимостей по путям ранга 0, есть

,

то есть все дуги и все пути нулевой длины (пути без промежуточных вершин).

Сейчас будет доказана теорема о том, что метод последовательного исключения неизвестных для решения системы (1) дает действительно наименьшее решение системы. Условно назовем этот метод методом Гаусса по аналогии с классическим методом решения числовых систем линейных уравнений. Мы увидим, что в процессе прямого хода алгоритма последовательно вычисляются стоимости путей возрастающих рангов, а в итоге значение неизвестной  определиться как стоимость прохождения из -й вершины графа в заключительную вершину , после чего обратный ход алгоритма даст стоимости прохождения в заключительную вершину из всех вершин графа, что и означает вычисление наименьшего решения системы (1).

Рассмотрим первый шаг «прямого хода» процедуры Гаусса. После подстановки выражения (2) во все уравнения системы (1) (начиная со второго) и приведения подобных членов получим:

 (3) при .

Обозначим через  коэффициент при  в -ом уравнении. Ясно, что  есть не что иное, как стоимость прохождения из вершины  в вершину  по всем путям ранга, не большего 1, т.е. по всем путям, промежуточной вершиной которых может быть только вершина . Свободный же член -ого уравнения, обозначаемый , есть стоимость прохождения из вершины  в вершину  по всем путям ранга, не большего 1.

По индукции легко доказать, что на -ом шаге процедуры прямого хода получим уравнение относительно :

,

где

,



суть стоимости прохождения из вершины  в нее же и в вершину соответственно по всем путям ранга, не большего .

Тогда наименьшее решение этого уравнения



есть не что иное, как стоимость прохождения из вершины  в вершину  по всем путям ранга, не большего , т.е. по всем путям. Но эта стоимость есть -ая компонента наименьшего решения системы (1). Следовательно, в процессе вычислений «обратного хода» процедуры Гаусса мы получим наименьшие значения остальных неизвестных, т.е. метод последовательного исключения неизвестных действительно дает наименьшее решение системы (1).

**Теорема 6**. Метод последовательного исключения неизвестных как метод решения системы (1) дает наименьшее решение системы.

**Замечания**. 1. В выражении для стоимости по путям ранга не большего 1, так как матрица стоимостей по путям нулевого ранга равна  должна стоять итерация суммы *a*11+1, но она как нетрудно понять, совпадает с итерацией самого элемента *a*11.

2. В приведенном выше доказательстве используется, конечно, и то, что вершина не может быть промежуточной вершиной какого-либо пути – по построению нашего графа.

Рассмотренное доказательство позволяет понять, что «метод Гаусса» решения систем линейных уравнений в замкнутых полукольцах есть модификация метода вычисления матрицы стоимостей размеченного орграфа через вычисление матриц стоимостей по путям различных рангов. Кроме того, понятно, что метод распространяется на полукольца с итерацией.

# Заключение

Основной результат статьи – доказательство теоремы, согласно которой метод последовательного исключения неизвестных при решении систем линейных уравнений в полукольцах с итерацией (в частности, в замкнутых полукольцах) дает наименьшее решение системы. В процессе доказательства устанавливается связь между этим методом («методом Гаусса» для полуколец) и методом вычисления матрицы стоимостей для размеченного орграфа путем последовательного вычисления матриц стоимостей по путям возрастающих рангов. Оказывается, что эти два метода являются разными модификациями одного и того же алгоритма. В установлении такой связи состоит научная новизна результатов статьи.

Помимо изложенного в статье предлагается также методически обоснованная последовательность изложения элементов теории полуколец, а именно, доказываются важные свойства так называемой бесконечной суммы, на которых основана разрешимость линейных уравнений и систем линейных уравнений в полукольцах с итерацией, затем доказывается замкнутость полукольца с итерацией относительно решений линейных систем. Некоторые доказательства пересмотрены и существенно упрощены. В некоторых случаях более подробно рассматриваются детали, обычно опускаемые в учебных руководствах. В этом состоит методическое значение полученных результатов.

## Список литературы

1. *Варанкина В.И., Вечтомов Е.М.* Функциональные алгебры и полукольца: результаты исследований 2016 года // Математический вестник педвузов и университетов Волго-Вятского региона. 2017, №19. – С. 36-53
2. *Чермных В.В.* Полукольцо натуральных чисел как базовая модель изучения полуколец //Вестник Вятского гуманитарного университета. 2012. Т.3, №1. – С. 62-65.
3. *Izhakian Z., Rowen L., Knebusch M.* Categories of Layered Semirings // Communications in Algebra. 2015. Vol. 43. N 5. – P. 1807-1836.
4. *Beasley L.B., Song S.-Z.* Linear Operations that Preserve Term Ranks of Matrix over Semirings // Bulletin of the Malaysian Mathematical Society. 2014. Vol. 37, № 3.- P. 719-726.
5. *Katsov Y., Nam T.G., Zumbragel J.* On Simpleness of Semirings and Complete Semirings // Journal of Algebra and its Applications. 2014. Vol. 13, N 6.- P. 145-150.
6. *Shmatkov V.D.* Semiring Isomorphisms and Automorphisms of Matrix Algebras // Journal of Mathematical Sciences. 2017. – P. 1-7.
7. *Вечтомов Е.М.* Полукольца и их применения // Математический вестник педвузов и университетов Волго-Вятского региона. 2014. № 16. – С. 67-72.
8. *Вечтомов Е.М., Варанкина В.И.* Полукольца и их применения. III // Математический вестник педвузов и университетов Волго-Вятского региона. 2015. № 17. – С. 54-66.
9. *Алешников С.И., Болтнев Ю.Ф., Език З., Ишанов С.А, Куих В.* Формальные языки и автоматы VII: формальные ряды деревьев (часть I)// Вестник Балтийского федерального университета им. И. Канта. Серия: Физико-математические и технические науки. 2011. №10. – С. 5-32.
10. *Алешников С.И., Болтнев Ю.Ф., Език З., Ишанов С.А, Куих В.* Формальные языки и автоматы V: пары полукольцо-полумодуль Конвея и конечные автоматы // Вестник Балтийского федерального университета им. И. Канта. Серия: Физико-математические и технические науки. 2009. №10. – С. 6-42.
11. *Никулина Н.С.* Полукольцо перечисления всех простых путей в графе // Математический вестник педвузов и университетов Волго-Вятского региона. 2011. №13.- С. 132-136.
12. *А.И. Белоусов, С.Б. Ткачев*. Дискретная математика. – 5-е изд. - М.: Изд-во МГТУ им. Н.Э. Баумана, 2015. – 744 с.
13. *Вечтомов Е.М., Петров А.А.* Полукольца с идемпотентным умножением // Вестник Сыктывкарского университета, Серия 1: Математика, Механика, Информатика. 2011. №14. – С. 21-32.
14. *Блюмин С.Л., Жбанов С.А.* Идемпотентная математика: некоторые предпосылки и приложения //Вестник высших учебных заведений Черноземья. 2011, №2.- С. 41-45.
15. *Чупраков Д.В.* Криптографические алгоритмы над абстрактными полукольцами // Электронные информационные системы. 2016, №3(10).- С. 90-96.
16. *Николаев Д.А.* Динамические системы с двумерным параметром над идемпотентными полукольцами для моделирования движения мультиагентных систем // Системы управления и информационные технологии. 2012. Т. 48, №2. – С. 22-26.
17. *Вечтомов Е.М.* Курс по выбору «Функциональная алгебра и полукольца» для аспирантов // Современные проблемы науки и образования. 2015. №2-2.- С. 318.
18. *Kuich W.* Automata and Langueges Generalised to ꙍ-continues Semirings // Theoretical Comput. Sci. 1991. № 79. – P. 137-150.
19. *Белоусов А.И.* О методике изложения некоторых разделов теории формальных языков: леммы о разрастании // Инженерный вестник. МГТУ им. Н.Э. Баумана. Электрон. журн. 2015, №12. Режим доступа: <http://engbul.bmstu.ru/doc/828263.html> (дата обращения: 23.12.15).