ТРУДЫ
МАТЕМАТИЧЕСКОГО ЦЕНТРА
ИМЕНИ Н. И. ЛОБАЧЕВСКОГО

ТОМ 55

ЛОБАЧЕВСКИЕ ЧТЕНИЯ – 2017

Материалы Шестнадцатой молодежной школы-конференции (Казань, 24 – 29 ноября 2017 г.)

Казанское математическое общество
2017

УДК 51+533
ББК 22.1 – 22.1
Т78

Печатается по рекомендации Редакционно-издательского совета Казанского математического общества

Составитель
А.А. Агафонов

Научный редактор
С. Р. Насыров

Т78 Труды Математического центра имени Н. И. Лобачевского. Т.55. Лобачевские чтения – 2017: материалы Шестнадцатой молодежной научной школы-конференции (Казань, 24-29 ноября 2017 г.) / сост. А.А. Агафонов. – Казань: Из-во Казан. ун-та, 2017. – 172 с.

ISBN 978-5-00019-912-1 (Т.55)
ISBN 978-5-00019-263-4

Сборник содержит материалы Шестнадцатой молодежной научной школы-конференции «Лобачевские чтения – 2017», организованной на базе Института математики и механики им. Н. И. Лобачевского Казанского (Приволжского) федерального университета. Школа-конференция проведена в Казани с 24 по 29 ноября 2017 года.

Книга предназначена для научных работников, преподавателей, аспирантов и студентов, специализирующихся в различных областях математики, механики и их приложений.

УДК 51+533
ББК 22.1 – 22.1

ISBN 978-5-00019-912-1 (Т.55)
ISBN 978-5-00019-263-4

УДК 539.3

МОДЕЛИРОВАНИЕ НЕЛИНЕЙНЫХ ДЕФОРМАЦИЙ С УЧЕТОМ КОНТАКТНОГО ВЗАИМОДЕЙСТВИЯ

А.И. Абдрахманова[1], Л.У. Султанов[2]

1 *a061093@mail.ru*; Казанский(Приволжский) федеральный университет, Институт математики и механики им. Н.И. Лобачевского

2 *lenar.sultanov@kpfu.ru*; Казанский(Приволжский) федеральный университет, Институт математики и механики им. Н.И. Лобачевского

В статье предлагается методика численного исследования напряженно-деформированного состояния упругих тел в условиях их контактного взаимодействия на основе метода конечных элементов. Исследование вопросов контактного взаимодействия твердых тел представляется весьма актуальной проблемой в связи с тем, что одним из наиболее распространенных на практике способов передачи внешних усилий является контактное взаимодействие. Контактная задача решается с применением метода конечных элементов. Для выполнения условий контакта при конечно-элементной реализации используется метод штрафа. В качестве алгоритма поиска зоны контакта используется алгоритм проекции ближайшей точки. Применение данных подходов предполагает использование итерационных методов решения.

Ключевые слова: упругие деформации, контактное взаимодействие, метод штрафа, алгоритм проекции ближайшей точки, контактный конечный элемент.

Кинематика описывается левым тензором Коши–Грина (мера деформации Фингера), тензором пространственного градиента скорости и тензором деформации скорости. Физические соотношения задаются с помощью функции упругого потенциала. Напряженное состояние описывается тензором истинных напряжений Коши–Эйлера, который определяется в актуальном состоянии. Вводится удельная потенциальная энергия деформации, которая зависит от левого тензора Коши–Грина.

Для решения задачи применяется метод шагового нагружения. В качестве базового уравнения принимается вариационное уравнение мощностей в актуальном состоянии. После линеаризации получена разрешающая система линейных алгебраических уравнений, где неизвестным является приращение перемещений в текущем времени.

Для выполнения условий контакта при конечно-элементной реализации применяется метод штрафа, в соответствии с которым дополнительные условия для контактных условий вводятся локально на элементе. Для нормального контакта без трения формируется функционал, основанный на функции проникновения. Функционал содержит параметр штрафа, увеличение которого приводит в пределе к удовлетворению условий по не проникновению тел друг в друга. Контактный функционал добавляется к функции упругого потенциала для двух тел.

Для поиска зоны контакта применяется алгоритм проекции ближайшей точки. Сформулированная в вариационной постановке с применением данного подхода контактная задача является нелинейной и для решения применяется итерационный метод Ньютона.

Численная реализация основана на методе конечных элементов, на базе восьмиузлового полилинейного элемента. Контактный элемент аппроксимируется пятиузловым конечным элементом. Построены все необходимые соотношения для вычисления подынтегральных выражений в виде зависимостей от скоростей.

Ниже приводится решение задачи Герца о взаимодействии бесконечного цилиндра с плоскостью. В качестве конечно-элементной сетки была выбрана сетка с высокой концентрацией элементов в зоне контакта, и чуть более разреженной в областях, не подверженных непосредственному контакту. Ниже представлено деформированное состояние цилиндра и распределение контактных напряжений во всем теле

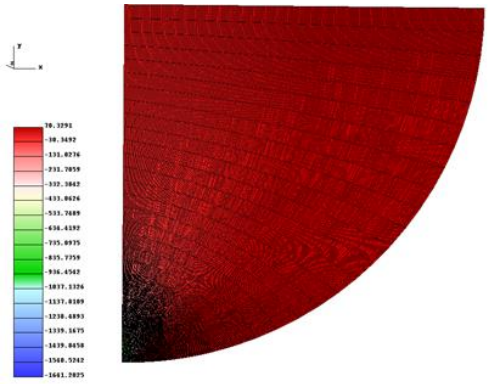


Рис. 1. Распределение контактных напряжений

и в области контакта:

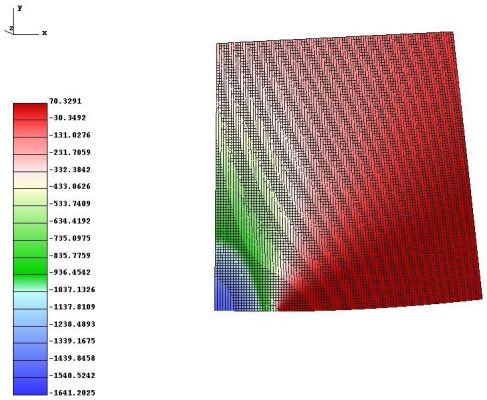


Рис. 2. Распределение контактных напряжений в области контакта

Также приводится решение контактной задачи о вдавливании прямоугольного штампа с плоским основанием в упругое полупространство, нижнее основание которого также ограничено абсолютно жесткой плоскостью.

Решенные тестовые геометрически нелинейные задачи демонстрируют работоспособность предложенной методики. Произведен расчет напряженно-деформированного состояния и контактного давления, при сравнении с аналитическими данными которых мы получаем совпадение с приемлемыми погрешностями.

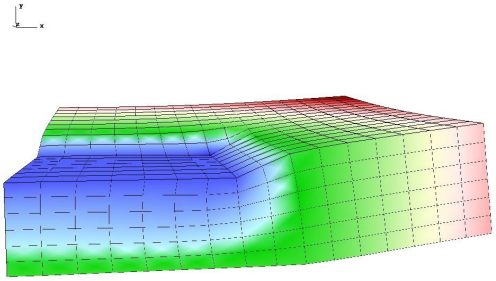


Рис. 3. Деформированное состояние упругой плиты, ограниченной жесткой поверхностью и сдавленной жёстким штампом

Результаты получены в рамках выполнения государственного задания Минобрнауки России (9.9786.2017/8.9).

Литература

1. Konyukhov A., Izi R. *Introduction to computational contact mechanics: a geometrical approach.* – John Wiley and Sons Ltd, 2015. – 302 с.

2. Голованов А. И., Султанов Л. У. *Теоретические основы вычислительной нелинейной механики деформируемых сред.* – Казань, 2008. – 164 с.

NUMERICAL MODELLING OF FINITE DEFORMATIONS WITH CONTACT INTERACTION

A.I. Abdrakhmanova, L.U. Sultanov

In the paper a method of numerical investigation of the stress-strain state of elastic solids with contact interaction is presented. To perform the contact conditions in finite element implementation the method of penalty is used, under which additional conditions for contact conditions are imposed locally on the element, which leads to the possibility of constructing the so-called contact elements locally. For normal contact without friction is formulated functionality based on functions of the penetration. The contact functionality is add to the function of elastic potential for the two bodies. To search the contact area, we use "the closest point projection algorithm". This algorithm allows building the contact elements, based on the approach called "master-slave". The contact problem, formulated in a variational form, with the use of these approaches, is nonlinear and to solve this problem, we apply Newton's iteration method. The results were obtained under the state assignment of the Russian Ministry of Education and Science (9.9786.2017/8.9).

Keywords: finite deformations, contact interaction, penalty method, closest point projection algorithm, contact element.

УДК 519.67

МОДЕЛЬ ЭЛЕКТРОХИМИЧЕСКОГО ПРОЦЕССА В ЖИДКОМ ДИЭЛЕКТРИКЕ С РАЗДЕЛЯЮЩЕЙ СЕЛЕКТИВНОЙ МЕМБРАНОЙ

И.А. Авдеев[1]

1 *avdeyev.iv@gmail.com*; Кубанский государственный университет, факультет математики и компьютерных наук

В статье обсуждается построение математической модели для процесса переноса заряженных частиц через селективную мембрану в жидком диэлектрике, а также решение прикладной задачи по определению значений напряжения и тока во внешней цепи при известных сопротивлении во внешней цепи и концентрациях ионов в рабочей камере.

Ключевые слова: селективная мембрана, диэлектрик, ионообмен, электрическое поле, поток ионов, напряжение, сила тока, сопротивление.

Рассмотрим селективную мембрану, выполненную в форме тонкой плоской пластины из диэлектрического материала. Погрузим её в некоторый водный раствор. Всё пространство, в котором находится раствор, делится вертикально расположенной мембраной на две камеры: левую и правую. Левую камеру условно назовём анодной, а правую – катодной. Селективность мембраны проявляется в том, что сквозь неё фильтруются лишь положительно заряженные ионы. Поместим в анодную и катодную камеры электроды, замкнутые через внешнюю цепь. Для простоты будем считать, что электроды представляют собой бесконечные плоские пластины, расположенные параллельно мембране. Выберем цилиндрическую плоскую поверхность с образующей, параллельной оси O_x и поперечным сечение площади S. Эта цилиндрическая поверхность ограничивает в пространстве между электродами область, представляющую собой гальванический элемент. Предполагается, что при разности потенциалов U и сопротивлении r во внешней цепи течёт ток I. Нас будет интересовать, какое напряжение U и ток I во внешней цепи мы сможем получить при определенных концентрациях ионов в рабочей камере и известном сопротивлении внешнего участка r. Подвижность ионов u считается известной. Подчеркнём, что нас интересует исключительно стационарный процесс. Если пренебречь конкретикой окислительно-восстановительных реакций и связанных с ними скачками электрического поля на электродах, то при некоторых дополнительных предположениях получается достаточно простая модель, в которой показатели напряжения и тока во внешней цепи восстанавливаются по падению концентраций внутри рабочей камеры. Всё что при этом потребуется. – это знание коэффициентов диффузии и подвижности ионов во всех трёх областях: в анодной и катодной камерах, а также в толще мембраны. Определение концентраций сводится к решению трансцендентного уравнения. Характеристика u транспортных свойств мембраны при этом предполагается заранее известной. Тогда можно сформулировать основные положения модели:

1. В электролите возникает потенциал двойного слоя с локализацией на мембране.
2. Любая область внутри анодной или катодной камеры сохраняет свою электриче-

скую нейтральность.
3. Потенциал электрического поля непрерывен на границе электродов.

Непрерывность потенциала электрического поля на границе электродов означает выполнение равенства

$$\Delta\Phi = U,$$

а чисто диффузионный характер движения ионов в рабочих камерах приводит к частному случаю уравнения потока:

$$j = -D\frac{d[c]}{dx}.$$

Так как мы изучаем стационарный процесс, то концентрация $[c]$ в соответствующих областях представляется линейной функцией. Получаем два уравнения, отдельно для анодной камеры и катодной камеры

$$\frac{h_a}{D_a}j = [ox] - [c_a],$$
$$\frac{h_k}{D_k}j = [c_k] - [red].$$

В таком случае уравнение для напряжения принимает вид:

$$U = \mu \ln \frac{[c_a] + \frac{hj}{uU}}{[c_k] + \frac{hj}{uU}}. \tag{1}$$

С целью определения предельных значений тока и напряжения во внешней цепи кажется целесообразным ввести средние по рабочим камерам значения концентраций:

$$[c_1] = \frac{[ox] + [c_a]}{2}, \quad [c_2] = \frac{[red] + [c_k]}{2}, \quad [c_1] \geq [c_2].$$

Перенос ионов в толще мембраны происходит лишь вследствие диффузионного механизма, поле Å оказывает тормозящее действие на движение ионов в толще мембраны. Если разомкнуть внешнюю цепь, с течением времени плотность потока j будет равна нулю, а значит сам процесс перейдет в равновесное состояние.

Выражение для ЭДС источника имеет вид:

$$U_{xx} = \mu \ln \frac{[c_1]}{[c_2]}.$$

Теперь найдем величину I_{kz}. Для этого воспользуемся соотношением (1), которое с учётом закона Ома для внешней цепи можно переписать и перейти к пределу при $r \to 0$. В результате получим величину $I_k z$:

$$I_{kz} = \frac{DnFS}{h}([c_k^*] - [c_a^*]).$$

Эти предельные характеристики тока и напряжения являются вспомогательными, позволяют найти сопротивление источника для использование далее в задаче, а

также ограничивают соответствующие характеристики внешней цепи. Из закона Ома следует:

$$U + I\frac{\mu}{2nFS}\left(\frac{h_a}{D_a} + \frac{h_k}{D_k}\right)\frac{\ln\frac{[c_1]}{[c_2]}}{[c_1]-[c_2]} = \mu \ln\frac{[c_1]}{[c_2]}.$$

Если объединить все эти уравнения в одно, то для него можно сформулировать теорему о существовании и единственности решения:

Теорема. *При условии* $[c_1] > [c_2]$ *уравнение имеет, и при том единственное, решение* $(I, U) \in (0, I_{kz}) \times (0, U_{xx})$.

На аноде имеет место реакция: $O_2 + 4H + 4e^- = 2H_2O$. Это означает, что в результате восстановительной реакции выделяется элементарный заряд, который совершает необходимую работу во внешней цепи. Стоит отметить особую важность зависимости абсолютной диэлектрической проницаемости среды и подвижности иона водорода от температуры среды рабочих камер, это связано с явлением сверх подвижности иона водорода при высоких температурах. Предполагается, что следние концентрации $[c_1]$ и $[c_2]$ известны, и $[c_1] > [c_2]$

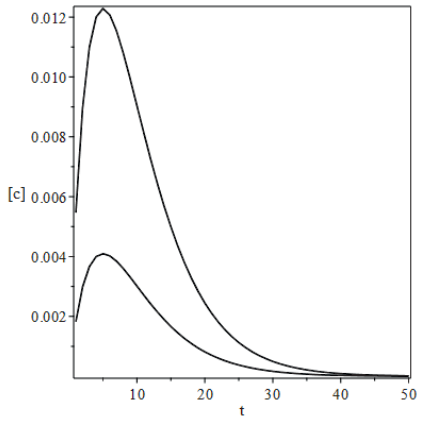


Рис. 1. Изменение средних концентраций ионов в камерах

В результате были получены следующие значения для тока

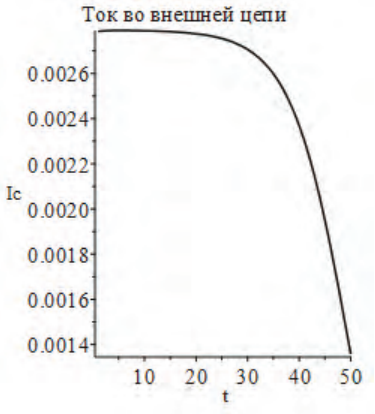


Рис. 2. Ток во внешней цепи

Литература

1. Джексон Дж. *Классическая электродинамика*. – М.: Мир, 1965.

2. Таланов В.М., Житный Г.М. *Ионные равновесия в водных растворах*. – М.: Академия естествознания, 2007.

3. Мартинсон Л.К., Смирнов Е.В. *Физика в техническом университете, т.5. Квантовая физика*. – М.: МГУ, 2012.

4. Заболоцкий В.И., Никоненко В.В. *Перенос ионов в мембранах*. – М.: Наука, 1996.

MATH MODEL OF AN ELECTROCHEMICAL PROCESS IN A LIQUID DIELECTRIC WITH A SEPARATING SELECTIVE MEMBRANE

I.A. Avdeyev

This paper discusses the construction of a math model for the process of transfer of ions through the selective membrane in a liquid dielectric, and finding the solutions of amperage and voltage, obtained from known external impedance and concentrations of the ions in the cells.

Keywords: selective membrane, dielectric, ion exchange, electric potential, ionic current, voltage, amperage, impedance.

УДК 517.9

О ЗАДАЧЕ КОШИ ДЛЯ ОБЫКНОВЕННОГО ДИФФЕРЕНЦИАЛЬНОГО УРАВНЕНИЯ С ДРОБНОЙ ПРОИЗВОДНОЙ В ГЛАВНОЙ ЧАСТИ

Ю.Р. Агачев[1], А.В. Гуськова[2]

1 *jagachev@gmail.com*; Казанский (Приволжский) федеральный университет, Институт математики и механики им. Н.И. Лобачевского

2 *avsavina@kpfu.ru*; Казанский (Приволжский) федеральный университет, Институт математики и механики им. Н.И. Лобачевского

В статье исследуется задача Коши для одного класса линейных обыкновенных дифференциальных уравнений с дробной производной в главной части в случае, когда известные коэффициенты уравнения принадлежат классу Гельдера. Доказана корректность задачи в специальным образом построенной паре функциональных пространств. На основе аппарата алгебраических полиномов построены приближения к точному решению исследуемой задачи.

Ключевые слова: линейное уравнение, дробно–дифференциальное уравнение, задача Коши, корректная постановка, приближенное решение.

Пусть m – фиксированное натуральное число, вещественное число α подчинено условию $m-1<\alpha<m$.

В работе исследуется задача Коши

$$x^{(i)}(a)=0, \quad i=\overline{0,m-1}, \tag{1}$$

для дифференциального уравнения дробного порядка вида

$$Kx \equiv (D^{\alpha}_{a+}x)(t) + \sum_{i=1}^{m} p_i(t)x^{(m-i)}(t) = y(t),\ a < t \le b, \tag{2}$$

где $p_i(t), y(t)$ — известные, $x(t)$ — искомая функции на $[a,b]$; $D^{\alpha}_{a+}x$ есть левосторонняя производная Римана—Лиувилля (см., например, в [1, с. 44]) порядка α функции $x(t)$:

$$(D^{\alpha}_{a+}x)(t) \equiv \frac{1}{\Gamma(m-\alpha)}\frac{d^m}{dt^m}\int_a^t \frac{x(\tau)d\tau}{(t-\tau)^{\alpha-m+1}}, \tag{3}$$

$\Gamma(\cdot)$ — гамма-функция.

Существование этой производной обеспечивается условием

$$\int_a^t \frac{x(\tau)\,d\tau}{(t-\tau)^{\alpha-m+1}} \in AC^{m-1}[a,b],$$

где $AC^{m-1}[a,b]$ означает класс функций $f(t)$, имеющих на $[a,b]$ абсолютно непрерывную производную $f^{(m-1)}(t)$ порядка $m-1$ $(f^{(m-1)} \in AC[a,b] \equiv AC^0[a,b])$. Поскольку искомая функция $x(t)$ в задаче (1), (2) имеет производную порядка $m-1$, известные свойства дробных производных позволяют преобразовать формулу (3):

$$(D^{\alpha}_{a+}x)(t) \equiv \frac{1}{\Gamma(1-\{\alpha\})}\frac{d}{dt}\int_a^t \frac{x^{(m-1)}(\tau)d\tau}{(t-\tau)^{\{\alpha\}}} = (D^{\{\alpha\}}_{a+}x^{(m-1)})(t), \tag{4}$$

где $\{\alpha\}$ – дробная часть числа α.

Пусть $H_\beta \equiv H_\beta[a,b]$ – пространство функций, удовлетворяющих на $[a,b]$ условию Гельдера с показателем $\beta, 0 < \beta < 1$. Через $H_{0,\beta}$ обозначим его подпространство функций, обращающихся в нуль в точке a. Норму в пространстве H_β введем обычным образом:

$$\|f\|_\beta = \|f\|_C + H(f;\beta),\ f \in H_\beta.$$

Здесь $\|f\|_C$ – обычная max-норма в пространстве непрерывных на отрезке $[a,b]$ функций, $H(f;\beta)$ – наименьшая постоянная Гельдера функции $f \in H_\beta$.

Введем в рассмотрение оператор дробного интегрирования Римана—Лиувилля $I^{\{\alpha\}}_{a+}$ порядка $\{\alpha\}$. Этот оператор, как известно, осуществляет взаимно-однозначное соответствие $H_{0,\beta}$ на $H_{0,\{\alpha\}+\beta}$, если $0 < \beta < \{\alpha\} + \beta < 1$. Тогда дробно—дифференциальный оператор $D^{\{\alpha\}}_{a+}$ переводит пространство $H_{0,\{\alpha\}+\beta}$ на $H_{0,\beta}$.

Определим пару пространств, в которой будем рассматривать исходную задачу. Пусть $Y = H_{0,\beta}$, $X = \widetilde{W}^{m-1}H_{0,\{\alpha\}+\beta}$ – пространство функций, удовлетворяющих условиям (1) и имеющих на $[a,b]$ производную порядка $m-1$, принадлежащую $H_{0,\{\alpha\}+\beta}$. Норму в пространстве X зададим по формуле

$$\|x\|_X = \|x^{(m-1)}\|_{\{\alpha\}+\beta},\ x \in X.$$

В паре пространств (X,Y) задачу (1), (2) запишем в операторной форме

$$Kx \equiv Dx + Gx = y\ (x \in X, y \in Y), \tag{5}$$

где, с учетом формулы (4),

$$(Dx)(t) = (D_{a+}^{\{\alpha\}} x^{(m-1)})(t),\ (Gx)(t) = \sum_{i=1}^{m} p_i(t) x^{(m-i)}(t).$$

Справедлива следующая

Теорема 1. *Пусть вещественное число γ удовлетворяет условию $\{\alpha\} + \beta < \gamma \le 1$ и выполнены предположения:*

1) $p_i \in H_{0,\gamma}[a,b], i = \overline{1,m}$;

2) $y \in H_{0,\beta}[a,b]$.

Тогда уравнение (5) (а, следовательно, и задача (1), (2)) в паре (X,Y) корректно поставлена по Адамару.

Заметим, что для дробной производной порядка α имеют место [1, с. 44] соотношения $(D_{a+}^{\alpha} x)(a) = 0$, если $x(t) = (t-a)^{\alpha-i}$, $i = 1,2,\ldots,[\alpha]+1$. С учетом этого свойства для дробных производных, приближенное решение уравнения (5) будем искать в виде

$$x_n(t) = (t-a)^{\alpha} \sum_{i=0}^{n} c_i t^i, \tag{6}$$

Пусть H_n есть подпространство алгебраических полиномов степени не выше n. Во введенных выше пространствах введем подпространства: X_n – подпространство обобщенных полиномов вида (6), $Y_n = H_n$. Пусть $P_n : Y \to Y_n$ – произвольно фиксированный оператор проектирования Y на Y_n.

Будем решать задачу (1), (2) общим полиномиальным проекционным методом, согласно которому неизвестные коэффициенты полинома (6) определяются из уравнения

$$K_n x_n \equiv Dx_n + P_n G x_n = P_n y \quad (x_n \in X_n). \tag{7}$$

Отметим, что при конкретном выборе оператора проектирования P_n будем получать вычислительные схемы того или иного проекционного метода, в частности, методов Галеркина, коллокации, подобластей.

С помощью результатов по общей теории приближенных методов функционального анализа (см., например, [2, гл. I]) доказывается следующая

Теорема 2. *Пусть γ – вещественное число, удовлетворяющее условию $\{\alpha\} + \beta < \gamma \le 1$, и выполнены предположения:*

1) $y, p_i \in H_{0,\gamma}[a,b], i = \overline{1,m}$;

2) $P_n^2 = P_n$, $\|P_n\|_{C\to C} = O(\ln n)$;

3) задача (1), (2) имеет единственное решение $x^*(t)$ при любой правой части из $H_{0,\beta}$.

Тогда уравнение (7) при всех натуральных n, начиная с некоторого, однозначно разрешимо. Приближения, найденные по формуле (6), сходятся по норме пространства X к точному решению со скоростью

$$\|x^* - x_n\|_X = O\left\{\frac{\ln n}{n^{\gamma-\beta}}\right\}.$$

Отметим, что результаты сохраняют силу, если в уравнении (2) добавлены слагаемые с младшими производными дробного порядка. Кроме того, при наличии

у коэффициентов уравнения (2) дополнительных свойств гладкостного характера скорость сходимости найденных приближений к точному решению возрастает. Последнее вытекает из одного результата по приближению функций алгебраическими полиномами в пространствах гельдеровых функций (см., например, [3]).

Литература

1. Самко С. Г., Килбас А. А., Маричев О. А. *Интегралы и производные дробного порядка и некоторые их приложения.* – Минск.: Наука и техника, 1987. – 688 с.

2. Габдулхаев Б. Г. *Оптимальные аппроксимации решений линейных задач*. – Казань.: Изд-во Казан. ун-та, 1980. – 232 с.

3. Agachev J. R., Galimyanov A. F. *On Justification of General Polynomial Projection Method for Solving Periodic Fractional Integral Equations* // Lobachevskii Journal of Mathematics. – 2015. – Vol. 36, No. 2. – P. 97-102.

ON THE CAUCHY PROBLEM FOR AN ORDINARY DIFFERENTIAL EQUATION WITH A FRACTIONAL DERIVATIVE IN THE PRINCIPAL PART

J.R. Agachev, A.V. Guskova

The article studies the Cauchy problem for a class of linear ordinary differential equations with fractional derivative in the main part, in the case when known coefficients of the equation belong to the class of Holder. The correctness of the problem in a special way constructed pair of function spaces is proved. Approximations to exact solution of the investigated problem is constructed on the basis apparatus of algebraic polynomials.

Keywords: linear equation, fractional differential equation, Cauchy problem, correct statement, approximate solution.

УДК 517.968

О КОРРЕКТНОЙ ПОСТАНОВКЕ ОБЩЕЙ КРАЕВОЙ ЗАДАЧИ ДЛЯ УСЛОВНО КОРРЕКТНЫХ ИНТЕГРО-ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ ФРЕДГОЛЬМА–ВОЛЬТЕРРА

Ю.Р. Агачев[1], М.Ю. Першагин[2]

1 *jagachev@gmail.com*; Казанский (Приволжский) федеральный университет, Институт математики и механики им. Н.И. Лобачевского

2 *mpershagin@mail.ru*; Казанский (Приволжский) федеральный университет, Институт математики и механики им. Н.И. Лобачевского

В работе исследуется общая краевая задача для линейных интегро-дифференциальных уравнений Фредгольма–Вольтерра, заданных на отрезке числовой прямой, в которых порядок внутреннего дифференциального оператора выше порядка соответствующего внешнего дифференциального оператора. Доказана корректная постановка указанной задачи в смысле Адамара в специальным образом выбранной паре невесовых пространств Соболева.

Ключевые слова: пространство Соболева, интегро-дифференциальное уравнение, общая краевая задача, корректная постановка.

В этой работе продолжаются исследования, начатые в [1]. Рассматривается общая краевая задача

$$R_i(x) = 0,\ i = \overline{0, m-1}, \tag{1}$$

для интегро-дифференциального уравнения

$$Kx \equiv x^{(m)}(t) + \sum_{i=1}^{m} \gamma_i(t) x^{(m-i)}(t) + \\ + \sum_{j=0}^{p} \left\{ \int_a^b h_j(t,s) x^{(j)}(s)\, ds + \int_a^t g_j(t,s) x^{(j)}(s)\, ds \right\} = y(t), \quad a \le t \le b. \tag{2}$$

Здесь R_i, $i = \overline{0, m-1}$, – заданные линейно-независимые функционалы, определенные на подпространстве $C^{(m-1)}[a,b]$ $(m-1)$–раз непрерывно-дифференцируемых на $[a,b]$ функций ($C[a,b] \equiv C^{(0)}[a,b]$), $\gamma_i(t)$, $i = \overline{1,m}$, $h_j(t,s)$, $g_j(t,s)$, $j = \overline{0,p}$, – известные функции в своих областях определения, $x(t)$ – искомая функция.

Целочисленные параметры m, p удовлетворяют условию $p > m \ge 0$, что влечет, по классификации Б.Г. Габдулхаева [2], условную корректность задачи (1), (2). Это означает, что (1), (2) может быть поставлена корректно по Адамару при определенных гладкостных свойствах коэффициентов уравнения (2).

Через $W^q L_2 \equiv W^q L_2[a,b]$, $q \in \mathbb{N}$, обозначим пространство функций, имеющих на $[a,b]$ производную порядка q, принадлежащую пространству L_2 квадратично-суммируемых функций. Норму в этом пространстве зададим обычным образом:

$$\|\varphi\|_{q,2} = \|\varphi\|_{L_2} + \left\|\varphi^{(q)}\right\|_{L_2} \qquad (\varphi \in W^q L_2). \tag{3}$$

Задачу (1), (2) будем рассматривать в паре пространств[1] (X, Y), где пространство правых частей $Y = W^{p-m} L_2$, пространство искомых элементов X состоит из функций, принадлежащих $W^p L_2$ и удовлетворяющих краевым условиям (1). В пространстве X норму согласуем с нормой в Y ((3) при $q = p - m$) по формуле:

$$\|x\|_X = \left\|x^{(m)}\right\|_{L_2} + \left\|x^{(p)}\right\|_{L_2} \equiv \left\|x^{(m)}\right\|_Y.$$

С введенными таким образом нормами пространства X и Y являются полными.

В паре (X, Y) задача (1), (2) может быть представлена в виде операторного уравнения

$$Kx \equiv Dx + \Gamma x + Hx + Gx = y \qquad (x \in X, y \in Y), \tag{4}$$

где операторы D, Γ, H, G задаются формулами:

$$(Dx)(t) \equiv x^{(m)}(t), \quad (\Gamma x)(t) \equiv \sum_{i=1}^{m} \gamma_i(t) x^{(m-i)}(t),$$

$$(Hx)(t) \equiv \sum_{j=0}^{p} \int_a^b h_j(t,s) x^{(j)}(s)\, ds, \quad (Gx)(t) \equiv \sum_{j=0}^{p} \int_a^t g_j(t,s) x^{(j)}(s)\, ds.$$

1 Для этого необходимо наложить на известные функции некоторые условия гладкостного характера.

Отметим, что оператор $D : X \to Y$ непрерывно обратим, причем

$$\|D\|_{X\to Y} = \|D^{-1}\|_{Y\to X} = 1.$$

Лемма 1 (см. в [1]). *Пусть выполнены предположения:*
1) $\gamma_i \in Y$, $i = \overline{1, m}$;
2) $h_j \in Y \times L_1$, $j = \overline{0, p-1}$;
3) $h_p \in Y \times L_2$.
Тогда оператор $\Gamma + H : X \to Y$ *вполне непрерывен.*

Далее, введем в рассмотрение функции $\psi_{j,k}(t) \equiv \frac{\partial^k}{\partial t^k} g_j(t,s)|_{s=t}$, $k = \overline{0, p-m-1}$, $j = \overline{0, p}$.

Лемма 2. *Пусть выполнены условия:*
1) $g_j \in Y \times L_1$, $j = \overline{0, p-1}$, $g_p \in Y \times L_2$;
2) $\psi_{j,k} \in W^{p-m-k-1}L_2$, $j = \overline{0, k+m+1}$, $k = \overline{0, p-m-2}$;
3) $\psi_{j,p-m-1} \in W^{p-m-k-1}L_2$, $j = \overline{0, p-1}$;
4) $\psi_{p,p-m-1} \in C[a,b]$;
5) $\psi_{j,k}(t) \equiv 0$, $j = \overline{k+m+2, p}$, $k = \overline{0, p-m-2}$.
Тогда оператор $G : X \to Y$ *вполне непрерывен.*

Леммы 1 и 2 дают достаточные условия корректной постановки задачи (1), (2).

Теорема. *Пусть выполнены предположения лемм 1 и 2 и задача (1) для уравнения* $x^{(m)}(t) = y(t)$ *имеет лишь нулевое решение. Тогда задача (1), (2) корректно поставлена по Адамару в паре пространств* (X, Y).

Утверждение теоремы вытекает из того факта, что при выполнении условий лемм 1 и 2 уравнение (4) является уравнением, приводящимся к уравнению второго рода с вполне непрерывным оператором. Следовательно, к уравнению (4) применима теория Фредгольма.

Замечание. Леммы 1 и 2 дают достаточные условия полной непрерывности операторов $\Gamma + H$ и G соответственно в случае, когда свойства функций h_j и g_j по каждой из переменных не зависят от другой переменной. Если же ядро интегрального оператора является разностным (в этом случае ядро задается функцией одного аргумента), то условия на это ядро будут задаваться через свойства гладкостного характера соответствующей функции одного аргумента.

Литература

1. Агачев Ю. Р., Першагин М. Ю. *Корректная постановка условно корректных интегро-дифференциальных уравнений в новой паре невесовых пространств Соболева* // Известия вузов. Математика. – 2017. – № 8. – С. 80–85.

2. Габдулхаев Б. Г. *Некоторые вопросы теории приближенных методов. II* // Известия вузов. Математика. – 1968. – № 10. – С. 21–29.

ON THE CORRECT FORMULATION
OF GENERAL BOUNDARY VALUE PROBLEMS FOR CONDITIONALLY WELL-POSED
INTEGRO-DIFFERENTIAL EQUATIONS OF FREDHOLM–VOLTERRA

J.R. Agachev, M.Yu. Pershagin

In this paper we investigate the general boundary-value problem for linear integrodifferential equations of Fredholm–Volterra, specified on a segment of the number line where the order of the internal differential operators is higher than that of the corresponding exterior differential operator. We prove well-posedness of this problem in the Hadamard sense in a specially selected pair of non-weighted Sobolev spaces.

Keywords: Sobolev space, integro-differential equation, general boundary-value problem, wellposedness.

УДК 517.928

МОДЕЛИРОВАНИЕ КРИТИЧЕСКИХ ЯВЛЕНИЙ В МОДЕЛИ ВОСПЛАМЕНЕНИЯ ГОРЮЧЕГО СПРЕЯ

А.Ж. Агатаева[1]

1 *aina2100@yandex.ru*; Самарский национальный исследовательский университет имени академика С.П. Королева

Работа посвящена геометрическому подходу к моделированию критических явлений в разнотемповых динамических моделях. Горение характеризуется наличием одновременно протекающих процессов с существенно различными скоростями (например, изменение температуры и расход реагирующего вещества), поэтому для моделирования таких явлений используются сингулярно возмущенные системы. На примере динамической модели воспламенения горючего спрея показано, что неустойчивые инвариантные многообразия сингулярно возмущенных систем могут применяться для моделирования критических явлений. Применение геометрической теории сингулярных возмущений позволило получить условия протекания критического режима в аналитической форме.

Ключевые слова: сингулярные возмущения, инвариантное многообразие, устойчивость, критические явления, тепловой взрыв.

1. Введение

В статье рассматривается процесс воспламенения горючего газа, содержащего капли жидкого топлива. Для моделирования критических явлений в рассматриваемой системе применен метод интегральных многообразий сингулярно возмущенных систем. Особенности горения и теплового взрыва в газовой среде, хорошо известны и широко представлены различными публикациями. Тем не менее, влиянию капель жидкости на динамику такого процесса уделялось меньше внимания. По существу, поведение таких систем обусловлено двумя процессами: потери тепла за счет испарения горючей жидкой среды (капель) и выделением тепла, связанного с экзотермической реакцией окисления в газовой фазе. На основе геометрической

теории сингулярно возмущенных систем изучена природа и получены условия протекания критических явлений в исследуемой химической системе.

2. Математическая модель

Математическая модель воспламенения горючего газа, содержащего капли жидкости, представляет собой систему нелинейных обыкновенных дифференциальных уравнений: уравнения энергии для реагирующего газа, массового уравнения для жидких капель и уравнения для концентрации горючего компонента газовой смеси. Модель построена при обычных для теории горения предположениях однородности химических процессов в каждой точке реакционного сосуда [1] и в безразмерной форме имеет вид [2]:

$$\gamma\frac{d\theta}{d\tau} = \eta\exp\left(\frac{\theta}{1+\beta\theta}\right) - \epsilon_1 r\theta(1+\beta\theta), \tag{1}$$

$$\frac{dr^3}{d\tau} = -\epsilon_1\epsilon_2 r\theta, \tag{2}$$

$$\frac{d\eta}{d\tau} = -\eta\frac{1}{1+\beta\theta}\exp\left(\frac{\theta}{1+\beta\theta}\right) + \epsilon_1 r\psi\theta. \tag{3}$$

где θ — безразмерная температура горючего газа, r — безразмерный радиус капли, η — безразмерная концентрация горючего газа, τ — безразмерное время, γ — безразмерный параметр, равный конечной безразмерной адиабатической температуре термически изолированной системы после взрыва, β — приведенная начальная температура, ϵ_1, ϵ_2 характеризуют взаимодействие между газовой и жидкой фазами, ψ — параметр, характеризующий отношение энергии сгорания газовой смеси к жидкой энергии испарения. Начальные условия для уравнений (1)-(3):

$$\theta = 0, \;\; \eta = 1, \;\; r = 1.$$

Соответствующая комбинация уравнений (1)-(3) и интегрирование по времени дает следующий интеграл энергии:

$$\eta - 1 + \frac{\gamma}{\beta}\ln(1+\beta\theta) + \frac{\psi-1}{\epsilon_2}(r^3-1) = 0, \tag{4}$$

что позволяет уменьшить порядок системы (1)-(3):

$$\gamma\frac{d\theta}{d\tau} = \left(1 - \frac{\gamma}{\beta}\ln(1+\beta\theta) - \frac{\psi-1}{\epsilon_2}(r^3-1)\right)\exp\left(\frac{\theta}{1+\beta\theta}\right) - \epsilon_1 r\theta(1+\beta\theta), \tag{5}$$

$$\frac{dr^3}{d\tau} = -\epsilon_1\epsilon_2 r\theta. \tag{6}$$

Таким образом, динамическое поведение системы зависит от пяти безразмерных параметров: $\beta << 1$, $\gamma << 1$, ϵ_1, ϵ_2, ψ. В работе [3] на основе анализа нулевого приближения медленного интегрального многообразия системы (медленной кривой) [4] установлено существование трех основных типов режимов химической реакции

в зависимости от значений дополнительных параметров системы. Такими режимами являются безопасный медленный режим горения, быстрый режим (режим типичного теплового взрыва) и режим теплового взрыва с задержкой. В последнем режиме есть фаза медленного разогрева системы перед тем, как процесс перейдет во взрывную фазу. Установлено существование критического режима, который разделяет области безопасных медленных режимов и взрывные процессы. Применение геометрической теории сингулярных возмущений позволяет получить условия протекания критического режима в аналитической форме. Для этого воспользуемся предложенными в [5] асимптотиками для траектории на участке срыва с медленного интегрального многообразия системы (5)-(6):

$$1 = r^* + \gamma^{\frac{2}{3}}\gamma_0^{\frac{2}{3}}\omega \operatorname{sign} f(r^*,\theta^*) + \frac{1}{3}\gamma \ln\frac{1}{\gamma}\gamma_1 \operatorname{sign} f(r^*,\theta^*) + O(\gamma), \tag{7}$$

и соответствующего значения бифуркационного параметра, в качестве которого рассмотрен параметр ϵ_1, где

$$\omega = 2.338107,\ \ \gamma_0 = \sqrt{\frac{2}{|g_{\theta\theta}(T)g_r(T)|}}|f(T)|,$$

$$\gamma_1 = \frac{6g_{\theta\theta}(T)f_\theta(T) - 2g_{\theta\theta\theta}(T)f(T)}{3g_{\theta\theta}^2(T)}.$$

Здесь T – точка срыва медленной кривой с координатами (r^*,θ^*):

$$\theta^* = 1 + 3\beta + ...,\ r^* = r_0^* + r_1^*\beta,$$

$$r_0^* = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},\ p = \frac{\epsilon_1\epsilon_2}{e(\psi-1)},\ q = \frac{\epsilon_2 + \psi - 1}{\psi - 1},$$

$$r_1^* = \frac{2e(\psi-1)(1 - r_0^{*3}) - 4\epsilon_1\epsilon_2 r_0^*}{\epsilon_1\epsilon_2 + 3e(\psi-1)r_0^{*2}}.$$

На рисунках 1,2 приведены результаты численного исследования системы (5)-(6) для критического режима. Особенностью критического режима является то, что он играет роль границы между безопасными и взрывными процессами. Кроме того, реализация такого режима позволяет получить сравнительно высокие значения температуры горючей смеси в рамках безопасного процесса.

3. Заключение

Впервые для рассматриваемой модели благодаря учету малых возмущений удалось установить существование критического режима разделяющего области безопасных реакций и опасных взрывных процессов. Применение геометрической теории сингулярных возмущений позволило также получить условия протекания критического режима в аналитической форме.

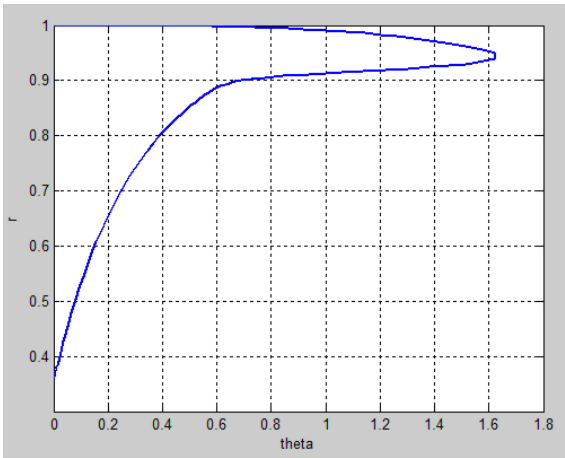


Рис. 1. Траектория системы в случае критического режима: $\epsilon_1 = \epsilon_1^*$, $\gamma = 0.01$, $\epsilon_1 = 2.2$, $\epsilon_2 = 0.8$, $\beta = 0.05$, $\psi = 0.19$.

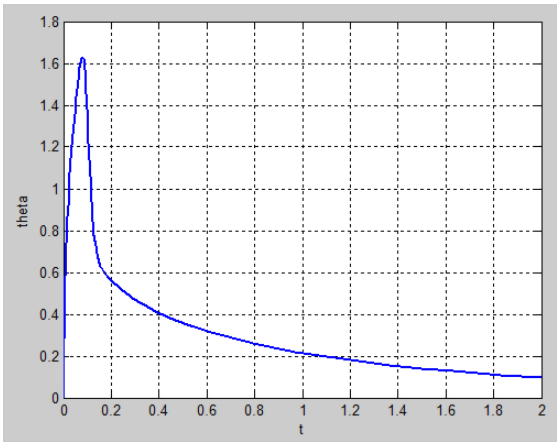


Рис. 2. Температура газа в случае критического режима: $\epsilon_1 = \epsilon_1^*$, $\gamma = 0.01$, $\epsilon_1 = 2.2$, $\epsilon_2 = 0.8$, $\beta = 0.05$, $\psi = 0.19$.

Литература

1. Semenov N.N. *Zur theorie des verbrennungs prozesses.* – Z. Physik. Chem., 1928. – P. 571-581.

2. Goldfarb I., Gol'dshtein V., Shreiber I., Zinoviev A. *Liquid Drop Effects on Self-Ignition of Combustible Gas* // Proceedings of the 26th Symposium (International) on Combustion. – 1996. – P. 1557–1563.

3. Agataeva A.Zh., Shchepakina E.A. *Critical conditions of ignition of fuel spray containing liquid fuel droplets* // CEUR Workshop Proceedings. – 2016. – P. 484–492.

4. Соболев В.А., Щепакина Е.А. *Редукция моделей и критические явления в макрокинетике.* – М.: Физматлит, 2010. – 320 с.

5. Мищенко Е.Ф., Розов Н.Х. *Дифференциальные уравнения с малым параметром и релаксационные колебания.* – М.: Наука, 1975. – 247 с.

MODELLING OF THE CRITICAL PHENOMENA IN THE MODEL OF FUEL SPRAY IGNITION

A.Zh. Agataeva

The work is devoted to a geometric approach of the modelling of critical phenomena in multi-rate dynamic models. The crucial idea of such approach is that the unstable invariant manifolds of singularly perturbed systems can be used for critical phenomena modelling. As an illustration a dynamic model of ignition of a fuel spray is considered. The application of the geometric theory of a singular perturbations allowed us to obtain the realizability conditions for the critical regime in analytical form.

Keywords: invariant manifold, singular perturbations, stability, critical phenomena, ignition, thermal explosion.

УДК 519.6

ХАОС В ДИНАМИКЕ КУСОЧНО-ЛИНЕЙНОГО ОТОБРАЖЕНИЯ С ДВУМЯ ПАРАМЕТРАМИ

И.И. Аксанова[1], Д.З. Уразова[2]

1 *ilsi050@mail.ru*; МБОУ «Высокогорская СОШ No 2»
2 *urazova.99@inbox.ru*; Казанский (Приволжский) федеральный университет

В работе проведено исследование динамической системы, заданной одномерным кусочно-линейным отображением f с двумя параметрами. Определены области значений параметров, при которых имеет место хаотическое поведение отображения f.

Ключевые слова: динамическая система, хаос, кусочно-линейное отображение.

В задачах прикладного характера все чаще применяют дискретные динамические системы, порожденные кусочно-линейными и кусочно-гладкими одномерными отображениями. Например, симметрическое и асимметрическое тентообразные отображения, заданные системой двух функций с одним или двумя параметрами. При этом анализируют чувствительность таких динамических систем к малым изменениям начальных условий и изучают хаотическое поведение заданного отображения. Такой анализ является актуальным, например, в робототехнике при разработке аналого-цифрового преобразователя для тактильных датчиков, при исследовании взаимодействия трейдеров на финансовых рынках [1–4].

Следующим естественным шагом является анализ математических моделей, представляющих собой дискретные динамические системы, определяемые кусочно-линейными отображениями, заданными с помощью трех или более линейных функций. Потребность в результатах таких исследований отмечается в некоторых недавних прикладных работах [4].

В работе исследована динамическая система, заданная одномерным кусочно-линейным отображением с двумя параметрами:

$$f(x)=\begin{cases} ax+1, & x\le 0,\\ (b-2)x+1, & 0\le x\le 1,\\ bx-1, & x\ge 1.\end{cases}$$

Это отображение является достаточно общим кусочно-линейным отображением, задаваемым тремя различными линейными функциями.

Плоскость — множество значений параметров (a,b) — была разбита на области с одинаковой динамикой, для каждой области проведено исследование динамического поведения отображения $f(x)$. Найдены условия существования неподвижных и двупериодических точек, определены области значений параметров a и b, где неподвижные точки и двупериодические орбиты являются притягивающими или отталкивающими. Построены паутинные диаграммы, соответствующие областям с различной динамикой отображения. Определены области значений параметров, при которых имеет место хаотическое поведение отображения $f(x)$.

Литература

1. Lindstrom T. *Dynamical properties of maps fitted to data in the noise-free limit* // Journal of Biological Dynamics. – 2013. – 7(1). – P. 108–116.

2. Jianxin Liu, Xuan Zhang, Zhiming Li, Xuling Li. *A tent map based conversion circuit for robot tactile sensor* // Journal of Sensors. – 2013. – V. 2013. – 5 p.

3. Wang Shuang-xin, Li Han, Zhang Xiu-xia, Wang Zhi-qin. *Nonlinear predictive load control of boiler-turbine-generating unit based on chaos optimization* // 2nd Chaotic Modeling and Simulation Int. Conf., – Crete, Greece, 1-5 June, 2009.

4. Tramontana F., Gardini L., Westerhoff F. *Intricate asset price dynamics and one-dimensional discontinuous maps* // In: Puu T., Panchuck A. (eds.) Advances in nonlinear economic dynamics. Nova Science Publishers, 2010.

CHAOS IN DYNAMICS OF PIECE-WISE LINEAR MAP WITH TWO PARAMETERS

I.I. Aksanova, D.Z. Urazova

We investigate a dynamic system given by a one-dimensional piece-wise linear map with two parameters. We describe domains in the plane of the parameters where dynamic behavior of the map is chaotic.

Keywords: dynamical system, chaos, piece-wise linear map.

УДК 517.9

РЕШЕНИЕ ЗАДАЧИ ШТУРМА–ЛИУВИЛЛЯ ДЛЯ ВОЛНОВОГО УРАВНЕНИЯ КОЛЕБАНИЙ ЖИДКОСТИ В ОГРАНИЧЕННОМ БАССЕЙНЕ ПЕРЕМЕННОЙ ГЛУБИНЫ

А.В. Багаев[1]

1 *a.v.bagaev@gmail.com*; Нижегородский государственный технический университет им. Р. Е. Алексеева

Обсуждается задача Штурма–Лиувилля для волнового уравнения колебаний малой амплитуды несжимаемой идеальной однослойной и двуслойной жидкости в замкнутом бассейне с неровным дном. Найдены собственные моды колебаний при определенной функциональной зависимости ширины и глубины бассейна. Показано, что собственные моды выражаются через многочлены Чебышева второго рода, и приведены некоторые свойства собственных мод. Построено решение задачи Коши в виде ряда по собственным модам колебаний, причем коэффициенты ряда могут быть вычислены как коэффициенты ряда Фурье по синусам.

Ключевые слова: волновое уравнение с переменными коэффициентами, уравнение Клейн–Гордона, задача Штурма–Лиувилля, многочлены Чебышева второго рода, колебания идеальной жидкости в замкнутом бассейне.

Исследуются колебания несжимаемой идеальной жидкости в канале прямоугольного сечения в рамках теории мелкой воды. Как известно [1], такие волновые движения описываются уравнением

$$B(x)\frac{\partial^2\eta}{\partial t^2} - \frac{\partial}{\partial x}\left(B(x)c^2(x)\frac{\partial\eta}{\partial x}\right) = 0, \qquad (1)$$

где $\eta(x,t)$ — смещение раздела слоев разной плотности в случае внутренних волн и водной поверхности в случае поверхностных волн, $c(x)$ — скорость распространения волн, $B(x)$ — ширина канала прямоугольной формы. Для поверхностных волн квадрат скорости распространения волн определяется равенством $c^2(x) = gh(x)$, где g — значение ускорения свободного падения, $h(x)$ — глубина бассейна, а для внутренних волн —

$$c^2(x) = g' \frac{h_1 h_2(x)}{h_1 + h_2(x)},$$

где h_1 и $h_2(x)$ — глубины верхнего и нижнего слоев, $g' = g(\rho_2 - \rho_1)/\rho_1$ — редуцированное значение ускорения свободного падения, $\rho_1 < \rho_2$ — плотности верхнего и нижнего слоев.

Метод разделения перменных, примененный к уравнениям вида (1), приводит к задаче Штурма–Лиувилля, решения которой удается найти только для некоторых частных случаев, причем, как правило, в виде специальных функций.

Трансформационная техника ([2]–[4]) позволяет перейти от гиперболического волнового уравнения (1) к уравнению Клейна–Гордона с постоянными коэффициентами, благодаря чему решение задачи Штурма–Лиувилля находится в элементарных функциях. Этот переход предполагает, что скорость распространения (следовательно, глубина) и ширина канала связаны уравнением

$$\frac{d}{dx}\left[\sqrt{\frac{c(x)}{B(x)}}\frac{d}{dx}(c(x)B(x))\right] = 2p\sqrt{\frac{B(x)}{c(x)}}, \tag{2}$$

тем самым общность исходной задачи сужается. Тем не менее, такие случаи интересны для физиков, поскольку позволяют доказать существование бегущих волн в сильно неоднородных средах [4]-[7].

В [8] получен общий вид решения уравнения (2) и проведен анализ полученных конфигураций бассейна. Некоторые такие частные конфигурации были получены в [7].

В [8] найдено ограниченное, но сингулярное решение ($c(x)$ или $B(x)$ обращаются в нуль). Такое решение соответствует конфигурации канала типа «озеро». Его можно записать в следующем виде

$$\begin{cases} c(x) = \sqrt{q}\dfrac{\sqrt{1-\psi^2(x)}}{\psi'(x)}, \\ B(x) = \dfrac{\gamma}{\sqrt{q}}\psi'(x)\sqrt{1-\psi^2(x)}, \end{cases} \tag{3}$$

где $\psi(x)$ — возрастающая непрерывная на $[0,L]$ и дифференцируемая на $(0,L)$ функция, L — длина канала, $q > 0$, $\gamma > 0$ — произвольные константы. Мы предполагаем, что $\psi(0) = -1$, $\psi(L) = 1$. Таким образом, $c(x)$ и $B(x)$ если и имеют особые точки, то только на концах отрезка $[0,L]$.

В [9] при естественном предположении ограниченности решения $\eta(t,x)$ уравнения (1) найдено выражение для n-ой собственной моды колебаний:

$$\eta_n(t,x) = A_n \cos(\omega_n t - \varphi) u_n(x),$$

где A_n, $\varphi = \text{const}$, $\omega_n = \sqrt{q}\sqrt{n^2-1}$ — частота колебаний,

$$u_n(x) = \frac{\sin(n \arccos \psi(x))}{\sqrt{1-\psi^2(x)}}.$$

Обозначив $s = \psi(x)$, функцию $u_n(x)$ можем переписать в виде

$$u_n(s) = \frac{\sin(n \arccos s)}{\sqrt{1-s^2}}, \quad s \in [-1,1]. \tag{4}$$

Формула (4) определяет в точности многочлен Чебышева второго рода $U_{n-1}(s)$ на отрезке $[-1,1]$ (см., например, [10]), благодаря чему функции $u_n(x)$ обладают рядом замечательных свойств [9].

Исследованы собственные моды для бассейнов следующих конфигураций: 1) постоянной ширины, 2) постоянной глубины, 3) «согласованного» канала переменных ширины и глубины.

1) Если канал имеет постоянную ширину, то согласно (3) скорость распространения $c(x)$ задается параметрически

$$\begin{cases} c(s) = c_0(1-s^2), \ c_0 = \text{const}, \\ x(s) = \dfrac{L}{\pi}\left(s\sqrt{1-s^2} + \pi - \arccos s\right), \end{cases} \quad s \in [-1,1].$$

При этом функции $u_n(x)$ также имеют параметрический вид

$$\begin{cases} u_n(s) = \dfrac{\sin(n \arccos s)}{\sqrt{1-s^2}}, \\ x(s) = \dfrac{L}{\pi}\left(s\sqrt{1-s^2} + \pi - \arccos s\right), \end{cases} \quad s \in [-1,1].$$

Отметим, что графики функций $u_n(x)$ касаются вертикальных прямых $x = 0$ и $x = L$. Таким образом, для этих функций «берег» является особой (сингулярной) точкой, где волновое поле, хотя и ограниченно, но его производная стремится к бесконечности.

2) В случае канала постоянной глубины ширина канала согласно (3) должна задаваться функцией $B(x) = B_0 \sin^2 \frac{\pi x}{L}$, $B_0 = \text{const}$, а функции $u_n(x)$ имеют явный вид

$$u_n(x) = (-1)^{n+1} \frac{\sin \frac{\pi n x}{L}}{\sin \frac{\pi x}{L}}.$$

В этом случае все моды описываются аналитическими функциями и на «берегах» они имеют нулевые производные.

3) Для случая «согласованного» канала переменных ширины и глубины $c(x)/B(x) = \text{const}$ скорость распространения $c(x)$ и ширина канала $B(x)$ согласно (3) определяются функциями

$$\begin{cases} c(x) = \dfrac{2c_0}{L}\sqrt{x(L-x)}, \ c_0 = \text{const}, \\ B(x) = \dfrac{2B_0}{L}\sqrt{x(L-x)}, \ B_0 = \text{const}. \end{cases}$$

В этом случае

$$u_n(x) = \frac{L}{2}\frac{\sin\left(n\arccos\frac{2x-L}{L}\right)}{\sqrt{x(L-x)}},$$

причем $u_n(x)$ является многочленом степени $n-1$ $\forall n \in \mathbb{N}$. В этом случае все собственные моды описываются аналитическими функциями и на «берегах» они имеют конечные ненулевые (кроме $n=1$) производные.

Показано, что решение задачи Коши для уравнения (1) с начальными условиями

$$\eta(x,0) = f_0(x), \quad \eta'_t(x,0) = f_1(x),$$

имеет вид

$$\eta(x,t) = C_1^{f_0} + \sum_{n=2}^{\infty}\left(C_n^{f_0}\cos\omega_n t + \frac{C_n^{f_1}}{\omega_n}\sin\omega_n t\right)u_n(x),$$

где

$$C_n^{f_i} = \frac{2}{\pi}\int_0^{\pi} f_i(x(y))\sin y \sin n y\, dy,\ i=0,1,\ n\in\mathbb{N},$$

являются коэффициентами разложения в ряд Фурье по синусам функции $f_i(x(y))\sin y$ на отрезке $[0,\pi]$, а функция $x = x(y)$ находится из уравнения $\psi(x) = \cos y$. Отметим, что в силу монотонности $\psi(x)$ уравнение $\psi(x) = \cos y$ имеет решение, причем:

1) $x(y) = \frac{L}{\pi}(\cos y \sin y + \pi - y)$ для случая канала постоянной ширины;

2) $x(y) = \frac{L}{\pi}(\pi - y)$ для случая канала постоянной глубины;

3) $x(y) = \frac{L}{\pi}(1+\cos y)$ для случая «согласованного» канала переменных ширины и глубины $c(x)/B(x) = \text{const}$.

Заключение. Нами получены ограниченные собственные моды, что свидетельствует об их физической реализуемости. Сингулярность (там, где она появляется) проявляется только в величине производной от смещения, которая не несет физического смысла. И хотя задача Штурма-Лиувилля решается не со стандартными граничными условиями типа Неймана или Дирихле, она ставится корректно и ее решения описывают собственные моды ограниченного водного бассейна переменной конфигурации («озера»).

Литература

1. Ляпидевский В.Ю., Тешуков В.М. *Математические модели распространения длинных волн в неоднородной жидкости*. – Новосибирск: СО РАН, 2000. – 419 с.

2. Bluman G. *On mapping linear partial differential equations to constant coefficient equations* // SIAMJ. Appl. Math. – 1983. – V. 43. – P. 1259–1273.

3. Varley E., Seymour B. *A method for obtaining exact solutions to partial differential equations with variable coefficients* // Stud. Appl. Math. – 1988. – V. 78. – P. 183–225.

4. Grimshaw R., Pelinovsky D., Pelinovsky E. *Homogenization of the variable-speed wave equation* // Wave Motion. – 2010. – V. 47, № 12. – P. 496–507.

5. Пелиновский Е.Н., Талипова Т.Г. *Безотражательное распространение волн в сильно неоднородных средах* // Фунд. и прик. гидрофизика. – 2010. – № 3. – С. 4–13.

6. Петрухин Н.С., Пелиновский Е.Н., Бацына Е.К. *Безотражательные волны в атмосфере Земли* // Письма в ЖЭТФ. – 2011. – Т. 93, № 10. –С. 625–628.

7. Талипова Т.Г., Пелиновский Е.Н., Куркина О.Е., Рувинская Е.А., Гиниятуллин А.Р., Наумов А.А. *Безотражательное распространение внутренних волн в канале переменного сечения и глубины* // Фундам. и прик. гидрофизика. – 2013. – Т. 6, № 3. – С. 46–53.

8. Багаев А.В., Пелиновский Е.Н. *Конфигурация канала переменного сечения, допускающая безотражательное распространение внутренних волн в океане* // Журнал Средневолжск. матем. общ. – 2016. – Т. 18, № 3. – С. 127–136.

9. Багаев А.В., Пелиновский Е.Н. *Собственные моды колебаний в ограниченном бассейне переменной глубины* // Журнал Средневолжского математического общества. – 2017. – Т. 19, № 2. – С. 126–138.

10. Суетин П.К. *Классические ортогональные многочлены*. – М.: ФИЗМАТЛИТ, 2005. – 480 с.

A SOLUTION OF THE STURM–LIOUVILLE PROBLEM OF WATER OSCILLATIONS IN THE CLOSED BASIN OF VARIABLE DEPTH

A.V. Bagaev

The Sturm–Liouville problem for the wave equation of small amplitude oscillations of an incompressible ideal single-layer and two-layer fluid in a closed basin with uneven bottom is discussed. Eigenmodes of oscillations are found in the channel, the width and depth of which are functionally associated and vanish on a frontier of channel. It is shown that such eigenmodes are expressed through Chebyshev polynomials of the second kind. Some properties of the eigenmodes are found. The solution of the Cauchy problem is constructed in the form of series in the eigenmodes, the coefficients of series can be computed as the coefficients of the Fourier series for sine.

Keywords: variable-coefficient wave equation, Klein–Gordon equation, Sturm–Liouville problem, Chebyshev polynomials of the second kind, water oscillations in closed basin.

УДК 004.91

МЕТОД ИЗВЛЕЧЕНИЯ ТЕРМИНОВ В ЦИФРОВЫХ МАТЕМАТИЧЕСКИХ КОЛЛЕКЦИЯХ

Р.Р. Батыршина[1]

1 *r-batyrshina@mail.ru*; Казанский (Приволжский) федеральный университет, Институт математики и механики им. Н.И. Лобачевского

В работе рассматриваются существующие методы извлечения терминов. Представлен алгоритм их извлечения, основанный на методе использования математических тезаурусов. Метод реализован на языке Java.

Ключевые слова: кластеризация, извлечение терминов, тезаурус.

Извлечения терминов из научных документов играет важную роль в пополнении и в разработке различных терминологических ресурсов, в первую очередь математических тезаурусов и онтологий [1], [2]. Пополнение таких ресурсов вручную достаточно трудоемкая задача. Для облегчения данного процесса необходимо автоматизировать процесс извлечения терминов [2].

Методы для извлечения терминов, существующие на данное время, в работе [3] разделены на три группы. Первая группа: тематические модели, основанные на методах кластеризации текстов. Кластеризация – это группировка документов цифровой коллекции “похожих” на основе некоторой меры схожести. Как отмечено в [4], задача кластеризации заключается в том, чтобы все похожие документы помещались в один кластер, а не похожие документы гарантированно попадали в разные кластеры. В работе [3] предлагаются следующие методы построения тематических моделей: алгоритм K-средних и сферически K-средних, иерархическая агломеративная кластеризация, неотрицательная матричная факторизация. Вторая группа: вероятностные тематические модели. Представляют каждый документ в виде смеси подтем, в которой каждая подтема представляет собой некоторое вероятностное распределение над словами. В работе [3] рассматриваются следующие представители этой категории: метод вероятностного латентного семантического индексирования, латентное размещение Дирихле. Третья группа: базовая тематическая модель, в которой подтемы не выделяются и каждый документ рассматривается как отдельная подтема.

Рассмотрев методы, описанные выше, мы разработали свой алгоритм извлечения терминов, основанный на методе использования словаря. Нашей задачей было создание программы, которая могла бы возвращать найденные термины в тексте, а вместе словарь, по которому осуществляется поиск терминов. Программа реализована на языке Java, способна выполнять следующие действия:

– принимать на вход имя файла (файл формата .txt, .pdf), а возвращать его содержимое в виде строки;

– выполнять поиск терминов в тексте с помощью созданного нами математического словаря. Метод основан на методе использования словаря, т. е. необходимо сделать проверку, входит ли слово из текста в словарь. Для того чтобы определить, соответствуют ли между собой слово из текста и термин, необходимо вычислить процентное соответствие. Вначале вычисляется процентное соответствие для слова – сколько процентов занимает префикс в слове. Затем, так же вычисляется процентное соответствие для термина. Если и у слова, и у термина префикс занимает 60 процентов – слова друг другу соответствуют. И раз слово из текста совпало термином, то возвращается пара слово — термин.;

– выделять найденные термины в самом тексте, добавляя к термину в скобках слово из словаря и возвращать текст в формате html;

– выписывать в отдельную таблицу все найденные термины в тексте.

С помощью следующих классов мы достигли реализацию вышеперечисленных действий:

TextLoader — класс, получающий текст из файла;

MatchedPair — класс пара – термин–слово;

MatchedPairInformation – пара – термин–слово, + позиция в тексте;

Dictionary – класс–словарь;

HtmlPreparer — класс, который находит термины в самом тексте и выделяет их желтым цветом, добавляя рядом со словом в скобках термин из словаря;

TermsMatcher – класс, который непосредственно выполняет поиск в словаре по тексту;

Main – запускает оконное приложение, загружает FXML–файл, получает словарь и отображает окно;

MainController – класс, отвечающий за окно;

Интерфейс программы представляет собой окно, в которое входят: форма для загрузки текста в программу, форма, отображающая загруженный текст, и форма с найденными терминами.

В дальнейшем предполагается улучшить программу с помощью алгоритма Кнута – Морриса – Пратта (алгоритм, осуществляющий поиск подстроки в строке), либо с помощью алгоритма Ахо – Корасик (алгоритм поиска подстроки).

Работа выполнена за счет средств субсидии, выделенной Казанскому федеральному университету для выполнения государственного задания в сфере научной деятельности, проект 1.2368.2017/ПЧ, и при частичной финансовой поддержке РФФИ и Правительства Республики Татарстан в рамках научного проекта №15–47–02472.

Литература

1. Елизаров А.М., Жильцов Н.Г., Кириллович А.В., Липачёв Е.К., Невзорова О.К. *Экосистема ONTOMATH и проект Всемирной цифровой математической библиотеки* // Труды межд. конф. по комп. и когн. лингвистике TEL-2016. — Казань: Изд-во Казан. ун-та, 2016. — С. 25–28.

2. Лукашевич Н.В. *Тезаурусы в задачах информационного поиска*. – М.: Изд-во МГУ, 2011.

3. Лукашевич Н.В., Нокель М.А. *Использование тематических моделей в извлечении однословных терминов* // CEUR-Workshop Proceedings. — 2013. — V. 1108. — P. 52-60. URL: http://ceur-ws.org/Vol-1108/paper7.pdf.

4. Ингерсолл Г.С., Мортон Т.С., Фэррис Э.Л. *Обработка неструктурированных текстов. Поиск, организация и манипулирование*. – ДМК Пресс, 2015.

5. Новикова Д.С. *Автоматическое выделение терминов из текстов предметных областей и установление связей между ними* // Конф. на РУДН, Инф.-тел. техн. и матем. моделир. высокотехн. систем. – 2012.

THE METHOD OF EXTRACTING TERMS IN THE MATHEMATICAL DIGITAL COLLECTIONS

R.R. Batyrshina

The paper considers existing methods of extracting terms. An algorithm for their extraction, based on the method of using the dictionary, is presented. The method is implemented in Java.

Keywords: clustering, extracting terms, dictionary.

УДК 519.688, 511.174

СТРУКТУРА ПЛОТНЫХ N-К И ЕЕ ВЫЧИСЛЕНИЕ

А. Большаков[1], А. Тимофеев[2], А.В. Рожков[3]

1 *aleksiosroller@mail.ru*; Кубанский государственный университет
2 *caesar147@mail.ru*; Кубанский государственный университет
3 *ros.seminar@bk.ru*; Кубанский государственный университет

Изучаются сгущения простых чисел — их количество, расположение на прямой, указываются их приложения для теории чисел и криптографии.

Ключевые слова: теория чисел, пакеты компьютерной алгебры, числа близнецы, простые числа.

Введение

Определение. *Множество из n простых чисел называется плотной n-кой (n-tuples), если они расположены на отрезке минимально возможной длины.*

Определение независимо введено в работах [1], [2]. Возможно это не единственные и не первые работы, где это очень естественное понятие определено. Плотная n-ка – это обобщение хорошо известных близнецов, т. е. простых чисел вида $(p, p+2)$, триплетов — простых чисел вида $(p, p+2, p+6)$ и $(p, p+4, p+6)$, сдвоенных близнецов — $(p, p+2, p+6, p+8)$. Дальнейшее построение плотных n-к нужно производить по индукции.

Алгоритм построения плотных n-к.

Пусть плотные n-ки уже построены построим $(n+1)$-ки. Допустим плотные n-ки разместились на отрезке $[p, p+2, \cdot, p+2k]$ длины $k+1$.

Рассматриваем отрезок $[p, p+2, \ldots, p+2k, p+2(k+1)]$ длины $k+2$.

Этап делителя 3. Рассматриваем числа $0, 2, 4, \ldots, 2(k+1)$ по модулю 3. Тут возможны два варианта. Число $k+1$ делится на 3.

Тогда у нас два подварианта. Из серединных чисел от 2 до $2k$ оставляем те, чей остаток от деления на 3 равен 1. Из серединных чисел оставляем те, что имеют остаток 2.

Если число $k+1$ не делится 3, то из серединных чисел оставляем те, что имеют остаток от деления на 3 равный 0 или $k+1$. На этом этап тройки завершен. Оставшиеся числа не образуют полную систему вычетов по модулю 3, и при правильном выборе начального числа p ни одно из них не будет делиться на 3.

Этап делителя 5. Получившиеся на предыдущем этапе числа рассматриваем по модулю 5. Пусть $S = \{0, 1, 2, 3, 4\} \backslash \{0, k+1 \mod 5\}$. Берем s из S и вычеркиваем все числа, имеющие остаток s, а остальные не трогаем. Так у нас возникнет 3 или 4 варианта. Этот этап нам гарантирует, что числа не будут делиться на 5, при соответствующем выборе числа p.

Этап делителя 7. К каждому варианту предыдущего этапа применяем тот же метод, что и на этапе делителя 5, только заменяем 5 на 7 и т.д. Вычеркивания производим до тех пор, пока у нас не останется ровно $n+1$ число, а последним этапом делителя будет максимальное простое число, не превосходящее число $n+1$. При

этом на некотором этапе может оказаться, что все оставшиеся числа делятся на текущий делитель. Тогда мы переходим к отрезку длины $k+3$ и повторяем процедуру. **Алгоритм** завершен.

Таким образом плотная n-ка или k-tuples [1] — это n чисел по модулю N (N — длина отрезка, внутри которого эти n чисел расположены), которые не образую полной системы вычетов ни по одному простому числу $p \leq N$.

В силу того, что вычисления приходится вести по все возрастающему числу простых модулей — нахождение структуры n-к весьма трудоемкая задача

Вложение плотных n-к друг в друга

В процессе вычислений были использованы идеи и методология, изложенная в работах [1], [2]. Вычисления производились с использованием пакета компьютерной алгебры gap 4.8.8. официальный адрес http://www.gap-system.org/

Условимся о некоторых обозначениях, упрощающих запись плотных n-к. Поскольку четное число не может быть простым, то все четные числа внутри отрезка длины N внутри которого заключена плотная n-ка мы будем опускать. Если некоторое нечетное место занято простым числом, мы это пометим цифрой 1, а 0 будет означать отсутствие числа.

В этих обозначениях упомянутые выше близницы, триплеты и сдвоенные близнецы примут вид

2-ки: (1,1). 3-ки: (1,1,0,1); (1,0,1,1). 4-ки: (1,1,0,1,1).

Приведем также вид плотных n-к до n=15 включительно. Отметим, что в настоящее время, октябрь 2017 г. найдены всего три 21-ки и ни одной 22-ки.

```
5-ки:       (1,1,0,1,1,0,1);
            (1,0,1,1,0,1,1).
6-ка:       (1,0,1,1,0,1,1,0,1).
7-ки:       (1,1,0,0,1,0,1,1,0,1,1);
            (1,1,0,1,1,0,1,0,0,1,1).
8-ки:       (1,0,0,1,1,0,0,1,0,1,1,0,1,1);
            (1,1,0,1,0,0,1,1,0,0,1,0,1,1);
            (1,1,0,1,1,0,1,0,0,1,1,0,0,1).
9-ки:       (1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,1);
            (1,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1);
            (1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1);
            (1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1).
10-ка:      (1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1).
11-ки:      (1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,1);
            (1,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1).
12-ки:      (1,0,0,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,1);
            (1,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,0,0,1).
13-ки:      (1,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,0,0,1,0,0,1);
            (1,0,0,1,0,0,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,1);
            (1,1,0,0,0,0,1,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1);
            (1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,1,0,0,0,0,1,1);
            (1,1,0,0,1,0,0,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1);
```

```
            (1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,0,0,1,0,0,1,1).
14-ки:      (1,1,0,0,1,0,0,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,1);
            (1,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,0,0,1,0,0,1,1)
15-ки:      (1,0,0,1,1,0,0,1,0,0,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,1);
            (1,1,0,1,0,0,1,1,0,0,1,0,0,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1);
            (1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,0,0,1,0,0,1,1,0,0,1,0,1,1);
            (1,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,0,0,1,0,0,1,1,0,0,1).
```

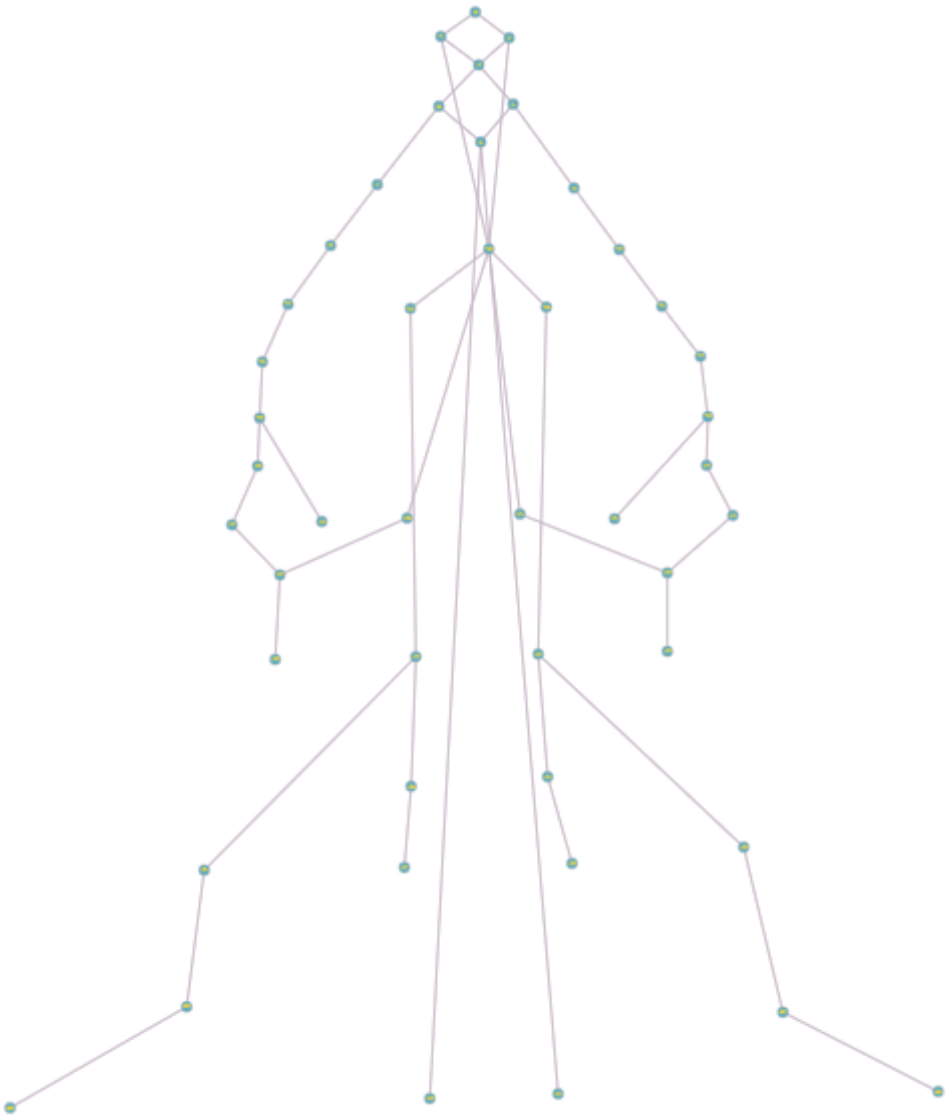


Рис. 1. Граф вложений плотных n-к до n < 20

Вычисление структуры плотной n-ки. Данные вычисления плохо поддаются распараллеливанию, поскольку чтобы вычислить структуру n-ки нужно знать структуру $(n-1)$-к. Затратив несколько сотен часов машинного времени нам удалось в 2013 г. вычислить структуру всех n-к до $n = 203$ включительно. В то же время, используя суперкомпьютеры, американский профессор из г. Мичиган Thomas J Engelsma со своей командой еще в декабре 2009 г. нашли структуру плотных n-к

до $n = 4507$ включительно http://www.opertech.com/primes/k-tuples.html. До $n = 203$ его и наши результаты полностью совпали. Следует отметить, что для данного n плотные n-ки могут иметь несколько различных структур, например, при $n = 105$ разных структур 105-к ровно 248.

Некоторые обобщения и выводы

Структура плотных n-к весьма интересна. Прежде всего для каждого n множество n-к симметрично, для каждой n-ки есть симметричная ей относительно середины отрезка, внутри которого она заключена.

Кроме того каждая n-ка содержит в себе по нескольку m-к при $m < n$. Подобное вложение имеет и большой практический смысл. Если мы нашли n-к для малых значений n, то для больших значений можно искать среди уже найденных. Мы приводим пример графа вложений плотных n-к для $n < 20$.

Точнее — это граф частично упорядоченного множества, у которого соединены ребрами только соседние элементы, в смысле упорядочения, а транзитивность — это движение по путям в графе. Сделано это для того, чтобы не перегружать граф ребрами. Но и даже в таком облегченном виде граф. на Рис. 1 выглядит весьма живописно. Обратим внимание, что его группа автоморфизмов элементарная абелева порядка 16.

Этот граф построен вручную. Следующая наша задача составить программу для построения графа вложений плотных n-к хотя бы до $n = 204$ — структур таких плотных n-к около 5 тыс.

Литература

1. Forbes T. *Prime clusters and Cunningham chains* // Math. Comp. – 1999. – V. 68, tom 228. – P. 1739–1747.

2. Рожков А.В., Рожкова М.В. *Локальная плотность множества простых чисел и апериодические коды* // Наука ЮУрГУ: Материалы 64-й научной конф. Секция техн. наук. – Челябинск: Изд-во ЮурГУ, 2012. – С. 86-90.

3. Рожков А.В. *Стратегия DPS - Debian-Python-Sage: Проблемно-ориентированные вычислительные среды на открытом коде* // Труды V междунар. науч.-практич. Конф. «Информационные технологии в образовании и науке» (ИТОН – 2016). – Казань: КФУ, 2016. – С. 172–179.

4. Рожков А.В., Рожкова М.В. *Экспериментальная (вычислительная) теория чисел* // Новые информационные технологии в образовании и науке: Материалы X межд. науч.-практ. конф., Екатеринбург, 27 февраля – 3 марта 2017 г. ФГАОУ ВО «Рос. гос. проф.-пед. ун-т». – Екатеринбург, 2017. – С. 413–417.

STRUCTURE OF DENSE K-TUPLES AND ITS CALCULATION

A. Bolchakov, A. Timofeev, A.V. Rozhkov

Condensations of prime numbers, their quantity, and the arrangement on the straight line are studied, their applications for the number theory and cryptography are specified.

Keywords: number theory, packages of computer algebra, number twins, prime numbers.

УДК 519.688, 511.174

ПЛОТНЫЕ N-КИ И ИХ ВЫЧИСЛЕНИЕ

А. Большаков[1], А. Тимофеев[2], А.В. Рожков[3]

1 *aleksiosroller@mail.ru*; Кубанский государственный университет
2 *caesar147@mail.ru*; Кубанский государственный университет
3 *ros.seminar@bk.ru*; Кубанский государственный университет

Изучаются сгущения простых чисел — их количество, расположение на прямой, указываются их приложения для теории чисел и криптографии.

Ключевые слова: теория чисел, пакеты компьютерной алгебры, числа близнецы, простые числа.

Введение

Определение. *Множество из n простых чисел называется плотной n-кой (n-tuples), если они расположены на отрезке минимально возможной длины.*

Определение независимо введено в работах [1], [2]. Возможно это не единственные и не первые работы, где это очень естественное понятие определено. Плотная n-ка - это обобщение хорошо известных близнецов, т.е. простых чисел вида $(p, p+2)$, триплетов — простых чисел вида $(p, p+2, p+6)$ и $(p, p+4, p+6)$, сдвоенных близнецов — $(p, p+2, p+6, p+8)$.

Таким образом плотная n-ка или k-tuples [1] — это n чисел по модулю N (N — длина отрезка, внутри которого эти n чисел расположены), которые не образуют полной системы вычетов ни по одному простому числу $p \le N$.

В силу того, что вычисления приходится вести по все возрастающему числу простых модулей — нахождение структуры n-к весьма трудоемкая задача

Следует отметить, что зная структуру плотной n-ки мы знаем только то, что если она существует, то имеет именно такой вид, но существование “живой” n-ки не гарантировано.

Ниже мы перечисляем некоторые плотные n-ки и указываем минимальное значение p, с которых эти n-ки начинаются. Условимся в записи n-ки символ p писать только вначале.

5-ки:	(p,2,6,8,12),	p = 1481;
	(p,4,6,10,12),	p = 1867.
6-ка:	(p,4,6,10,12,16),	p = 97.
7-ки:	(p, 2,8,12,14,18,20),	p = 5 639;
	(p, 2,6,8,12,18,20),	p = 165 701.
8-ки:	(p,6,8,14,18,20,24,26),	p = 88 793;
	(p,2,6,12,14,20,24,26),	p = 1 277;
	(p,2,6,8,12,18,20,26),	p= 15 760 091.
9-ки:	(p,4,10,12,18,22,24,28,30),	p = 74 266 249;
	(p,2,6,8,12,18,20,26,30),	p = 226 449 521;
	(p,4,6,10,16,18,24,28,30),	p = 113 143;
	(p,2,6,12,14,20,24,26,30),	p = 113 147.

Нахождение плотных n-к

В процессе вычислений были использованы идеи и методология, изложенная в работах [1], [2]. Вычисления производились с использованием пакета компьютерной алгебры gap 4.8.8. официальный адрес http://www.gap-system.org/

Зная структуру n-ки трудной задачей является непосредственное нахождение "живой n-ки" данной структуры. Эта задача легко поддается распараллеливанию - натуральный ряд разбивается на отрезки и на каждом из них ищется n-ка данной структуры. Используя около 20 компьютеров в 2013 г. нам удалось найти первую 14-ку, она оказалась 17-ти значной. Наименьшая 15-ка имеет 19 знаков, 16-ка - 21 знак, 17-ка 23 знака, 18-ка 25 знаков, 19-ка 27 знаков, 20-ка 29 знаков, первая 20-ка была найдена только в 2015 г. и самая маленькая 21-ка имеет тоже 29 знаков. В настоящее время 21-к найдено всего 3 штуки. В тоже время 22-к еще не найдено ни одной! Ознакомиться с последними достижениями в этой области можно по адресу https://sites.google.com/site/anthonydforbes/ktuplets.htm?attredirects=0

Вот основная программа по вычислению "живой" n-ки. Здесь две вспомогательные подпрограммы:

Rem — находит всех претендентов на число p — начало плотной n-ки, имеющей структуру M и претенденты выбраны по модулю — произведения всех первых m простых чисел.

All — проверяет, что все элементы n-ки со структурой M состоит из простых чисел.

Основная программа $T(S, M, m, n)$ использует эти программы на разных промежутках натурального ряда, а именно на промежутке (m, n).

```
Rem:=function(M,m)
local i,j,k,l,d,D,K,L,S;
l:=1; L:=[]; K:=[1]; D:=[]; S:=[];
for i in [1..m] do
l:= l*Primes[i];
L:= M mod Primes[i+1];
L:= Set(L);
L:= Difference([0..Primes[i+1]-1],L);
    for j in L do
        for k in K do
           d:=ChineseRem([l,Primes[i+1]],[k,Primes[i+1]-j]);
           Add(D,d);
od;
   od;
K:=Set(D);D:=[];
od;
S[1]:=K;
S[2]:=Length(K);
S[3]:=l*Primes[m+1];
 return(S);
end;
S:=Rem(M,m);;
```

```
All:=function(M,p)
local i,j,l;
for i in M do
    if IsProbablyPrimeInt(p+i) then  j:=true;
       else j:=false; break;
    fi;
od;
 return j;
end;

T:=function(S,M,m,n)
local t,q,s,l,L;
L:=[];
for  q in [m..n] do
    for  s in S[1] do t:= s +S[3]*q;
       if All(M,t) then
           Print(t,"\n");
           Add(L,t);
       fi;
   od;
od;

   return(L);
end;
```

Простые числа вездесущи в математике, особенно в криптографии [3]. Почти любой криптографический алгоритм начинается словами: “Пусть p – случайное простое число”. Число должно быть случайным и очень желательно расположенным в “общем положении”. Но если простое число оказалось принадлежащим, например, плотной 10-ке, то его положение окажется совсем не общим. В самом деле, рассмотрим типичное “криптографическое число”, содержащее 300 десятичных знаков. Согласно закону распределения простых чисел в районе 300-х значных чисел простым будет примерно каждое 700-е число. В тоже время в плотной 10-ке простым будет каждое 4-е число! Поэтому если мы случайно выбрали простое число из плотной n-ки, то его криптографическая ценность становится сомнительной.

Приложение из области абстрактной математики. Хорошо известна гипотеза Харди-Литлвуда, о том, что с удалением от начала координат локальная (а не только глобальная по закону П.Л. Чебышева) плотность распределения простых чисел уменьшается. Тем не менее, в плотной 447-ке плотность расположения простых чисел выше, чем в начале координат (см. http://www.opertech.com/primes/k-tuples.html). Проблема в том, что если плотная 447-ка и существует, то минимальный элемент в ней, возможно, имеет не менее 900 знаков в десятичной записи, поэтому нахождение ее до изобретения квантовых компьютеров весьма сомнительно.

Выводы

Даже не имея суперкомпьютеров исследовать плотные n-ки имеет смысл, и, более того, необходимо. Упомянутые выше вычислители занимаются рекордами, ищут все более и более многозначные n-ки, не интересуясь устройством этих сгущений простых чисел $\frac{n}{n!}$. показали, что даже в пределах до 10^{12} плотных 6-к примерно в 20 раз больше, чем предсказывает глобальный закон распределения простых чисел. Плотных 7-к в 100 раз больше, плотных 8-к в 1000 раз, плотных 9-к в 4000 раз больше, плотных 10-к в 5 тыс. раз и т.д.

Следует отметить, что пропорции количества реальных n-к к предсказанных глобальным законом распределения сохраняется на всех интервалах, которые нам удалось проверить от 10^6 до 10^{15} это рождает надежду, что подобное отношение является законом, а не эффектом начала координат.

Распределение плотных n-к – неких городов для простых чисел, может быть ключом для понимания законов локального распределения простых чисел, что очень важно и для теории чисел и для криптографии.

Литература

1. Forbes T. *Prime clusters and Cunningham chains* // Math. Comp. – 1999. – V. 68, tom 228. – P. 1739–1747.

2. Рожков А.В., Рожкова М.В. *Локальная плотность множества простых чисел и апериодические коды* // Наука ЮУрГУ: Материалы 64-й научной конф. Секция техн. наук. – Челябинск: Изд-во ЮурГУ, 2012. – С. 86-90.

3. Рожков А.В. *Стратегия DPS - Debian-Python-Sage: Проблемно-ориентированные вычислительные среды на открытом коде* // Труды V междунар. науч.-практич. Конф. «Информационные технологии в образовании и науке» (ИТОН – 2016). – Казань: КФУ, 2016. – С. 172–179.

4. Рожков А.В., Рожкова М.В. *Экспериментальная (вычислительная) теория чисел* // Новые информационные технологии в образовании и науке: Материалы X межд. науч.-практ. конф., Екатеринбург, 27 февраля – 3 марта 2017 г. ФГАОУ ВО «Рос. гос. проф.-пед. ун-т». – Екатеринбург, 2017. – С. 413–417.

5. Рожков А.В., Ниссельбаум О.В. *Теоретико-числовые методы в криптографии*. – Тюмень: ТюмГУ, 2007. – 160 с.

DENSE K-TUPLES AND THEIR CALCULATION

A. Bolchakov, A. Timofeev, A.V. Rozhkov

Condensations of prime numbers — their quantity, the arrangement on the straight line are studied, their appendices for the number theory and cryptography are specified.

Keywords: number theory, packages of computer algebra, number twins, prime numbers.

УДК 511.174

НЕКРИПТОГРАФИЧЕСКАЯ ХЭШ-ФУНКЦИЯ И СУММА ЦИФР СЛУЧАЙНОГО НАТУРАЛЬНОГО ЧИСЛА

А. Большакова[1], Д. Степанян[2], А.В. Рожков[3]

1 *anastaicha94@mail.ru*; Кубанский государственный университет
2 *diana14.02.94@mail.ru*; Кубанский государственный университет
3 *ros.seminar@bk.ru*; Кубанский государственный университет

Изучаются задачи теории чисел, которые могут быть модельными для других разделов математики.

Ключевые слова: теория чисел, пакеты компьютерной алгебры, криптография, простые числа.

Построение хэш-функции

Определение. *Функция χ, ставящая в соответствие сообщению произвольной длины сообщение фиксированной длины, называется хэш-функцией. Эквивалентно, отображение $\chi : \mathbb{N} \to \mathbb{N}$, имеющее конечный образ называется хэш-функцией. Хэш называется некриптографическим, если в процессе его создания не используется шифрование.*

Отметим, что весь мир использует некриптографический хэш. Российский ГОСТ Р 34.11–2012 хэш-функции с 2012 г. тоже стал некриптографическим.

Определение. *Функция $\psi : \mathbb{N} \to \mathbb{N}$ называется однонаправленной, если для любого $n \in \mathbb{N}$ образ $\psi(n) = m$ вычисляется за полиномиальное время, но не существует полиномиального алгоритма, вычисляющего прообраз n образа m.*

Проблема построения хэш-функций является одной из основных в криптографии. Нет математически строгих доказательств, что хоть одна из хэш-функций криптостойка. Именно поэтому весь мир пользуется одними и теми же алгоритмами — погибать так вместе!

Два наиважнейших свойства хэш-функции.

По хэшу должно быть очень трудно найти прообраз, т.е. хэш должен быть однонаправленной функций.

Должно быть очень трудно одновременно создать два разных сообщения с одним и тем же хэшем.

Чрезвычайная важность хэша в криптографии определяется тем, что во всех государственных системах электронной подписи шифруется не само сообщение, а его хэш.

Поэтому криптографы, математики и просто любители высоких технологий и трудных задач создают свои хэш-функции в надежде создать математически безупречный инструмент.

В нашей работе предложен хэш на основе простых арифметических понятий.

Пусть n – натуральное число, взятое в десятичной записи и $S(n)$ – сумма цифр этого числа.

Если к получаемым суммам последовательно применять функцию S, то в итоге получится некоторая цифра, принадлежащая множеству $J = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Функцию, которая ставит исходному натуральному числу эту итоговою цифру обозначим $\overline{S}:\mathbb{N}\to J$.

Лемма 1. *Пусть $n=j+9k$, $j\in J, k\in\mathbb{N}$ натуральное число, тогда, $\overline{S}(n)=j$.*

Лемма 2. *Следующие множества совпадают:*

$$J_3=\{\overline{S}(n^3), n\in\mathbb{N}\}=\{1,8,9\}.$$

Определение некриптографической хэш-функции. *Пусть некоторое сообщение закодировано натуральным числом M, тогда в качестве его хэша возьмем число $S(M^3)$.*

Для того чтобы подобрать сообщение M с заданным хэшем, например, 2017, нам необходимо найти такое натуральное число M, что $S(M^3)=2017$.

Учитывая то, как прихотливо ведет себя функция суммы цифр числа, решение подобной задачи весьма затруднительно.

Теорема 1. *Необходимым условием существования натурального числа M, такого, что $S(M^3)=n$, является включение $\overline{S}(n)\in J_3$.*

С другой стороны, если $n\in\{1+9k,8+9k,18k,9(6k-1)|k\in\mathbb{N}\}$, то искомое решение M существует.

Для чисел вида $n\in\{9(6k-5),9(6k-3)|k\in\mathbb{N}\}$ решение неизвестно.

О сумме цифр случайного натурального числа

Случайные числа играют в криптографии огромную роль – они являются основным инструментом при выборе ключа шифрования. Неверно, что математическое ожидание выбранной наугад цифры равно 9/2, а сумма цифр случайного n-значного числа равна $9n/2$.

Лемма 3. *Средневзвешенная цифра n-значного натурального числа равна* $9/2+1/2n$

Сумма цифр случайного n-значного натурального числа равна $9n/2+1/2$.

Теорема 2. *Средневзвешенная цифра числа, имеющего не более n знаков, равна*

$$\frac{9}{2}+\frac{9}{20}\cdot\frac{10^n}{10^n-1}\cdot\left(\frac{1}{1\cdot10^{n-1}}+\frac{1}{2\cdot10^{n-2}}+\ldots+\frac{1}{n\cdot10^9}\right).$$

Положим

$$S_n=\frac{9}{20}\cdot\left(\frac{1}{1\cdot10^{n-1}}+\frac{1}{2\cdot10^{n-2}}+\ldots+\frac{1}{n\cdot10^9}\right).$$

Теорема 3. *Для любого $n>1$ имеют место неравенства*

$$\frac{1}{2n}+\frac{1}{(2n)^2}>S_n>\frac{1}{2n}+\frac{1}{(2n)^3}.$$

Для $n>11$ верны неравенства

$$\frac{1}{2n}+\frac{1}{16n^2}>S_n>\frac{1}{2n}+\frac{1}{18n^2}.$$

Следствие 1.

$$\lim_{n\to\infty}\frac{S_n}{\frac{1}{2n}+\frac{1}{18n^2}}=1.$$

Следствие 2. *Для $n>11$ сумма цифр случайного не более чем n-значного числа принадлежит интервалу*

$$\left(\frac{9n+1}{2}+\frac{1}{18n},\frac{9n+1}{2}+\frac{1}{16n}\right).$$

Литература

1. Рожков А.В. *Стратегия DPS - Debian-Python-Sage: Проблемно-ориентированные вычислительные среды на открытом коде* // Труды V междунар. науч.-практич. Конф. «Информационные технологии в образовании и науке» (ИТОН – 2016). – Казань: КФУ, 2016. – С. 172–179.

2. Рожков А.В., Рожкова М.В. *Экспериментальная (вычислительная) теория чисел* // Новые информационные технологии в образовании и науке: Материалы X межд. науч.-практ. конф., Екатеринбург, 27 февраля – 3 марта 2017 г. ФГАОУ ВО «Рос. гос. проф.-пед. ун-т». – Екатеринбург, 2017. – С. 413–417.

3. Рожков А.В., Ниссельбаум О.В. *Теоретико-числовые методы в криптографии*. – Тюмень: ТюмГУ, 2007. – 160 с.

NOT CRYPTOGRAPHIC THE HASH FUNCTION AND SUM OF DIGITS OF RANDOM NATURAL NUMBER

A. Bolchakova, D. Stepanyan, A.V. Rozhkov

Number theory tasks which can be model for many sections of mathematics are studied.

Keywords: number theory, packages of computer algebra, cryptography, prime numbers.

УДК 511.174

ЗАМЕТКА О ПРОБЛЕМЕ КОЛЛАТЦА

А. Большакова[1], Д. Степанян[2], А.В. Рожков[3]

1 *anastaicha94@mail.ru*; Кубанский государственный университет
2 *diana14.02.94@mail.ru*; Кубанский государственный университет
3 *ros.seminar@bk.ru*; Кубанский государственный университет

Изучаются задачи теории чисел, которые могут быть модельными для других разделов математики.

Ключевые слова: теория чисел, пакеты компьютерной алгебры, криптография, простые числа.

Введение

Гипотеза Коллатца (гипотеза 3n+1, сиракузская проблема) — одна из нерешённых проблем математики.
Названа по имени немецкого математика Лотара Коллатца, сформулировавшего эту задачу 1 июля 1932 года.

Это сведения из Википедии (https://ru.wikipedia.org/wiki/%D0%93%D0%B8%D0%BF%D0%BE%D1%82%D0%B5%D0%B7%D0%B0_%D0%9A%D0%BE%D0%BB%D0%BB%D0%B0%D1%82%D1%86%D0%B0)

У Проблемы (гипотезы) в этом году юбилей — 85 лет.

Проблемой занимается масса энтузиастов, в основном, программистов, см. http://boinc.thesonntags.com/collatz/.

Цель нашего исследования проста и наивна, — проанализировать саму проблему, а не десятилетия ее обсуждения.

Определение 1. *Множество нечетных чисел обозначим $\mathbb{N}_1$, а множество нечетных чисел, не кратных 3, обозначим как $\mathbb{N}_3$.*

Определение 2. *Функция Коллатца K. Нечетному числу n ставится в соответствие нечетное число m, которое получено из числа $3n+1$ путем деления на максимально возможную степень числа 2. Таким образом $K : \mathbb{N}_1 \to \mathbb{N}_1$.*

Гипотеза Коллатца *Для любого нечетного числа m найдется такое натуральное n, что $K^n(m) = 1$.*

Лемма 1. $K(\mathbb{N}_1) \subseteq \mathbb{N}_3$.

Очевидно, ведь первое преобразование $n \rightarrowtail 3n+1$ и поэтому чисел, кратных 3 в образе быть не может.

Лемма 2. *$K(\mathbb{N}_3) = \mathbb{N}_3$, более того, каждый образ $m \in \mathbb{N}_3$ имеет бесконечно много прообразов в $\mathbb{N}_3$.*

Лемма 3. *Существуют сколь угодно длинные цепочки, подтверждающие гипотезу Коллатца.*

Пример. *Для любого натурального n имеет место равенство $K(2^n-1) = 3\cdot 2^{n-1} - 1$, поэтому длина цепочки до 1 не менее, чем n.*

Лемма 4. *Прообраз $K^{-1}(1)$ бесконечен и состоит из чисел $\{\frac{4^n-1}{3} | n \in \mathbb{N}\}$ или в двоичной записи $\{1, 101, 10101, 1010101, ...\}$*

Вычисления вероятностей

Формально, преобразование Коллатца умножает исходное число на 3, а деление гарантировано только на 2. Поэтому возникает ложное ощущение, что образы преобразования Коллатца могут расти до бесконечности.

Лемма 5. *Четное число делится в среднем на 4.*

В самом деле, вычислим на какую степень делится среднее четное число. Каждое первое делится на 2, т.е. степень 1, каждое второе еще дополнительно на 2, т.е. $\frac{1}{2}$, каждое четвертое еще дополнительно на 2, это $\frac{1}{4}$ и т.д. В итоге получаем сумму

$$1 + \frac{1}{2} + \frac{1}{4} + ... = 2.$$

Поэтому, в среднем, после преобразования Коллатца, исходное число m умножается на 3 и делится на 4, и значит станет равно 1 примерно через $\log_{4/3}(n)$ шагов.

Однако в процессе выполнения преобразований Коллатца могут возникнуть далеко не все четные числа.

Лемма 6. *Рассмотрим преобразование Коллатца как отображение $K : \mathbb{N}_3 \longrightarrow \mathbb{N}_3$, тогда только $\frac{2}{9}$ четных чисел могут появиться в цепочках Коллатца.*

В самом деле, это только числа вида $3(6k+1)+1 = 2(9k+2)$ и $3(6k+5)+1 = 2(9k+8)$, $k \in \mathbb{N}$.

Однако и четные числа такого вида тоже в среднем делятся на 4 и поэтому наша оценка длины цепочки как примерно равной $\log_{4/3}(n)$ не изменяется.

Преобразование Коллатца — это типичная цепь Маркова, когда следующий шаг зависит только от предыдущего. Рассмотрим два простейших случаю.

Первый случай. *Поскольку первая итерация преобразования Коллатца нас отправляет внутрь множества $\mathbb{N}_3$, то у нас есть только два вида нечетных чисел, с которыми нам нужно работать — это $6k+1$ и $6k+5$, $k \in \mathbb{N}$.*

Лемма 7. *Пусть у нас есть два состояния системы — это числа вида $6k+1$ и $6k+5$, $k \in \mathbb{N}$. Тогда матрица переходов марковского процесса имеет вид*

$$\frac{1}{3} \cdot \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

Это уже сразу матрица предельных переходов. При этом, как следует из леммы 7, в цепочках переходов преобразований Коллатца числа $6k+5$, $k \in \mathbb{N}$ встречаются в два раза чаще, чем числа вида $6k+1$, $k \in \mathbb{N}$.

Теперь рассмотрим числа нечетные числа по модулю 18. В этом случае множество $\mathbb{N}_3$ будет разбито на 6 подмножеств

$$18k+1, 18k+5, 18k+7, 18k+11, 18k+13, 18k+17, k \in \mathbb{N}. \quad (1)$$

Лемма 8. *Пусть у нас есть 6 состояний системы — это числа вида (1). Тогда матрица переходов марковского процесса имеет вид*

$$\frac{1}{63} \cdot \begin{pmatrix} 16 & 8 & 4 & 32 & 1 & 2 \\ 4 & 2 & 1 & 8 & 16 & 32 \\ 16 & 8 & 4 & 32 & 1 & 2 \\ 4 & 2 & 1 & 8 & 16 & 32 \\ 16 & 8 & 4 & 32 & 1 & 2 \\ 4 & 2 & 1 & 8 & 16 & 32 \end{pmatrix}$$

Эта матрица имеет характеристический многочлен $x^6 - x^5$ и жорданову форму из 5 жордановых клеток — 3 клетки с 0, одна с 1, и одна размера 2×2, с собственным значением 0.

При второй итерации, т.е будучи возведенной в квадрат, эта матрица становится матрицей предельных вероятностей — все ее строки становятся одинаковыми, равными строке

$$\frac{1}{63} \cdot (8, 4, 2, 16, 11, 22).$$

Таким образом, в траекториях действия преобразования Коллатца числа вида $18k+17$ встречаются в 11 раз чаще, чем числа вида $18k+7$. Это подтверждают и прямые вычисления до 1 миллиона (дальше не проверялось).

Просто вычисления

В процессе вычислений были использованы идеи и методология, изложенная в работах [1], [2], [3]. Вычисления производились с использованием пакета компьютерной алгебры gap 4.8.8. официальный адрес `http://www.gap-system.org/`.

Обширные вычисления до 10^9 и далее позволили выдвинуть гипотезы.

Гипотеза 1. *Пусть $n \in \mathbb{N}_3$ и $k(n)$ — длина преобразований Коллатца, превращающих n в 1, тогда для $n > 2 * 10^6$ имеет место неравенство*

$$\left|\frac{1}{n}\sum_{i=1}^{i=n} k(n) - 3,5 * \ln(n) - 1\right| < 0,2$$

Гипотеза 2. *Пусть $n \in \mathbb{N}_3$ и $k(n)$ — длина преобразований Коллатца, превращающих n в 1, тогда для $n > 1$ имеет место неравенство*

$$k(n) < 6 * 3,5 * \ln(n) = 21 \cdot \ln(n).$$

Литература

1. Рожков А. В. *Стратегия DPS - Debian-Python-Sage: Проблемно-ориентированные вычислительные среды на открытом коде* // Труды V-я Междунар. Науч.-практич. Конф. «Информационные технологии в образовании и науке» (ИТОН – 2016) Казань: КФУ, 2016. – С. 172-179.

2. Рожков А. В., Рожкова М. В.*Экспериментальная (вычислительная) теория чисел* // Новые информационные технологии в образовании и науке: материалы X междунар. науч.-практ. конф., Екатеринбург, 27 февраля – 3 марта 2017 г. ФГАОУ ВО «Рос. гос. проф.-пед. ун-т». – Екатеринбург, 2017. – С. 413-417.

3. Рожков А.В., Ниссельбаум О.В. *Теоретико-числовые методы в криптографии*. – Тюмень: ТюмГУ, 2007. – 160 с.

NOTE ABOUT KOLLATTS'S PROBLEM

A. Bolchakova, D. Stepanyan, A.V. Rozhkov

Number theory problems which can be model for many sections of mathematics are studied.

Keywords: number theory, packages of computer algebra, cryptography, prime numbers.

УДК 514.763.85

О ТОЧНОСТИ КОНСТАНТ В ОБОБЩЕННОМ НЕРАВЕНСТВЕ МАКАИ ДЛЯ ЖЕСТКОСТИ КРУЧЕНИЯ

Л.И. Гафиятуллина[1], Р.Г. Салахудинов[2]

1 *ligafiyatullina@kpfu.ru*; Казанский (Приволжский) федеральный университет, институт математики и механики им. Н.И. Лобачевского

2 *rsalakhud@gmail.com*; Казанский (Приволжский) федеральный университет, институт математики и механики им. Н.И. Лобачевского

В данной работе с использованием подходов из [3] доказывается обобщение неравенства Макаи для жесткости кручения в классе выпуклых областей.

Ключевые слова: жесткость кручения, моменты Евклида области относительно границы, изопериметрические неравенства, функция расстояния до границы области.

Ряд изопериметрических неравенств для жесткости кручения односвязных областей были получены Полиа и Сегё [2], Макаи [1], Пейном [4] и другими математиками.

Пусть G — выпуклая область на плоскости со спрямляемой границей и $\rho(z,G)$ — расстояние от точки z до границы ∂G области G.

Геометрический функционал, определяемый равенством

$$\mathrm{I}_p(G) := \iint\limits_{\Omega} \rho(z,G)^p \mathrm{dA},$$

называется моментом Евклида области G порядка p.

В 1962 г. Е. Макаи получил следующее неравенство

$$\mathrm{P}(G) \le 4\mathrm{I}_2(G),$$

справедливое для любой выпуклой области G.

Имеет место следующая

Теорема. *Пусть G – выпуклая область на плоскости и $p \ge 2$. Тогда имеет место следующее неравенство*

$$\mathrm{P}(G) \le \frac{(p+1)(p+2)}{3\rho(G)^{p-2}}\mathrm{I_p}(G) - \frac{(p-2)\mathrm{l}(\rho(G))\rho(G)^3}{3},$$

где $\mathrm{l}(\rho(G))$ — длина линии уровня $\rho(z,G)$, расположенной на расстоянии $\rho(G)$ от границы ∂G. Константы $(p+1)(p+2)/3$ и $(p-1)/3$ являются наилучшими из возможных.

Литература

1. Makai E. *On the Principal Frequency of a Membrane and the Torsional Regidity of a Beam* // Stanford University Press. – 1962. – P. 227-231.

2. Полиа Г., Сегё Г. *Изопериметрические неравенства в математической физике.* – М., Физматгиз, 1962. — 336 с.

3. Салахудинов Р.Г. *Изопериметрические свойства евклидовых граничных моментов односвязной области* // Изв. вузов. Математика. – 2013. – № 8. – С. 66-79.

4. Payne L.E. *Some isoperimetric inequalities in the torsion problem for multiply connected regions* / Studies in Mathematical analisis and Related Topics // Essays in honor of G. Polya (Standford University Press, Standford, California, 1962). – P. 270-280.

EXTENSIONAL OF MAKAI INEQUALITY FOR TORSIONAL RIGIDITY

L.I. Gafiyatullina, R.G. Salakhudinov

Using methods from [3], we proved a generalization of Makai inequality for convex region.

Keywords: torsional rigidity, Euclidian moments of a domain with respect to the boundary, isoperimetric inequalities, distance function to the boundary of a domain.

УДК 004.42

МЕТОД ФОРМИРОВАНИЯ СЕМАНТИЧЕСКОГО ПРЕДСТАВЛЕНИЯ ЦИФРОВЫХ МАТЕМАТИЧЕСКИХ ДОКУМЕНТОВ

П.О. Гафурова[1]

1 *polina_gafurova@yahoo.com*; Казанский (Приволжский) федеральный университет, Институт математики и механики им. Н.И. Лобачевского

Предложен метод семантического представления документов цифровых математической коллекции. Разработаны язык семантического описания документов коллекций, сервис по их обработке, инструменты семантического поиска и представления.

Ключевые слова: семантический веб, семантика, OMDoc, семантическое представление математических документов.

Работа является продолжением исследований, проведенных в [1], и посвящена разработке методов введения семантики в электронные математические документы на основе форматов OMDoc, sTEX и других (см., напр., [2], [3]).

Наличие большого количества источников обязывает представлять средства для обработки информации в сети интернет. Естественно, каждая сфера научного познания имеет особенности. В математике примером таких конструкций являются теоремы, леммы, доказательства, а главное – формулы. Данные конструкции имеют собственные значения и, следовательно, для машинной обработки необходимо включать в них некоторую скрытую информацию, в частности – метаданные. Для обработки математических документов необходимо привести их в семантический вид.

Введение семантики в Web является отличительной чертой Web 3.0. Элементы семантики можно встретить и сейчас, например, в немецкоязычной Wikipedia. Также в качестве примера можно отметить проект KWARK, нацеленный на внедрение семантики в различные документы, и в том числе математические [4], [5]. Для внедрения семантики в математические документы проект KWARK предлагает язык представления математических документов – OMDoc [2], [6]. OMDoc является по своей структуре XML документом с включенными в него математическими формулами. Данный формат был взят нами как основа для разработки языка семантического описания математических документов. Данный формат начал разрабатываться еще в 2000 году и до сих пор полностью не разработан, так как в математических документах существуют проблемы, которые пока решить не удалось [7]. Несмотря на то, что формат начал разрабатываться уже достаточно давно, нет работ, связанных с визуальным представлением документов на этом языке – язык является основой для некоторых других подпроектов проекта KWARK. Однако можно с помощью преобразований осуществлять вывод информации из файла на экран [1], [5].

Для семантического представления формул обычно используется язык MathML, также основанный на XML [8]. MathML работает не во всех браузерах, что затрудняет использование этого языка в качестве языка представления математических документов. Для этого при представлении математических документов

```
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xsl" href="matth.xsl"?>
<lib>
        <book id="1">
                <meta>
                        <author></author>
                        <title></title>
                        <year></year>
                        <publisher></publisher>
                </meta>
                <content>
                        <con id="1">
                                <contitle></contitle>
                                <desk id="1">
                                        <title></title>
                                        <sod></sod>
                                </desk>
                                <ax id="6">
                                        <title></title>
                                        <sod></sod>
                                </ax>
                                <theor id="7">
                                        <title></title>
                                        <sod></sod>
                                        <dok></dok>
                                        <altdok id="1"></altdoc>
                                        <altdok id="2"></altdoc>
                                        <sled id="1"></sled>
                                </theor>
                                <ex id="8">
                                        <title></title>
                                        <sod></sod>
                                </ex>
                                <lemm id="9">
                                        <title></title>
                                        <sod></sod>
                                </lemm>
                                <art id="10"></art>
                                ...
                        </con>
                        ...
                </content>
                <literat>
                        <bok id="1">
                                <num></num>
                                <ss></ss>
                        </bok>
                        ...
                </literat>
        </book>
        ...
<lib/>
```

Рис. 1. Схема семантического представления документа цифровой коллекции

в веб используют MathJax – язык, который не поддерживает семантику, однако воспроизводится всеми современными браузерами.

Для семантического описания цифровой математической коллекции нами предложен язык, основанный на XML (см., напр., [9]). Этот язык имеет следующую структуру: каждая книга описывается тегом <book> и заключает в себе: метаданные(теги <author>, <title>, <year>, <publisher>), а также тег содержания. В данном теге содержится основная информация по книге без потери структурной составляющей текста – параграфы и главы имеют свое строгое положение в тексте. В параграфах находятся содержательные теги для описания как математических структур: определение <def>, лемма <lemm>, теорема <theor>, аксиома <ax>, пример <ex>; так и не математических – тег <article>. Математические теги также имеют свое строгое местоположение и строение – в каждый математический объект включено краткое название, полный текст или альтернативный текст, также в случае с теоремами приведено доказательство, возможен случай приведения альтернативного доказательства и следствий.

Для передачи математических формул в созданном языке представления используется Presentation MathML (см., напр., [8], [10]). Однако, в связи с проблемами с отображением в браузерах, потребовалось решить задачу преобразования в

MathJax. Для этого было написано приложение на языке Python, которое при чтении из файла кода MathML выполняет преобразование в MathJax (результат на рис. 2). Данное приложение основано на использовании строгой структуры MathML при переформатировании его в MathJax.

```
<math>
<mfrac>
<mrow>
<mn>1</mn>
<mo>+</mo>
<msup>
<mo class="MathClass-op">sin</mo>
<mn>2</mn>
</msup>
<mfenced separators="" open="(" close=")">
<mi>x</mi><mo>+</mo><mi>y</mi></mfenced>
</mrow>
<mrow>
<mn>2</mn>
<mo>+</mo>
<mfenced separators="" open="|" close="|">
<mrow>
<mi>x</mi>
<mo>-</mo>
<mfrac>
<mrow><mn>2</mn><mi>x</mi></mrow>
<mrow>
<mn>1</mn>
<mo>+</mo>
<msup><mi>x</mi><mn>2</mn></msup>
<msup><mi>y</mi><mn>2</mn></msup>
</mrow>
</mfrac>
</mrow>
</mfenced>
</mrow>
</mfrac>
<mo>+</mo>
<mi>x</mi>
</math>
```

```
$\frac{1+\sin^{2}(x+y)}{2+|x-\frac{2x}{1+x^{2}y^{2}}|}+x $
```

Рис. 2. Входные данные и результат работы программы

Следующим шагом является создание веб – приложения на языке PHP с целью вывода документов коллекции на экран и семантического поиска по ним.

Веб-приложение отображает две страницы – первая страница выбора категории и термина (Рис. 3).

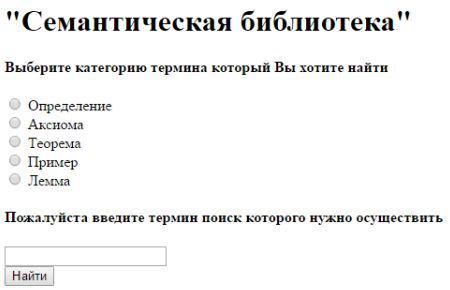
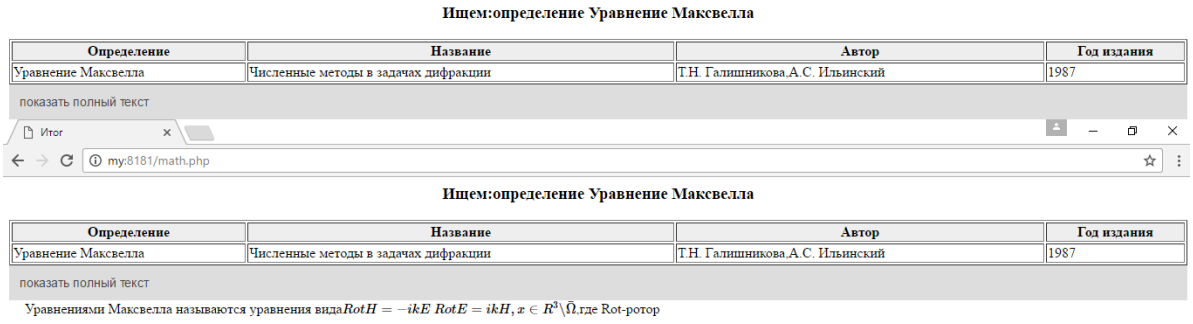


Рис. 3. Страница выбора категории и термина

В списке необходимо выбрать в какой категории пользователь хочет совершить поиск, а также вбить в текстовое поле поисковый запрос и нажать на кнопку. Далее происходит поиск по выбранной пользователем категории.

Вторая страница является страницей вывода. При выводе сначала указывается какой термин и из какой категории мы искали. Рис. 4 приведен как результат поиска: выводится название термина, метаданные по документу, такие, как название документа, автор или авторы, год издания. Имеется возможность отображения полного текста, описывающего термин. Данная информация скрыта для пользователя при обычном просмотре. В случае, когда было найдено два или более термина, выводятся все данные термины.



Ищем:определение Уравнение Максвелла

Определение	Название	Автор	Год издания
Уравнение Максвелла	Численные методы в задачах дифракции	Т.Н. Галишникова,А.С. Ильинский	1987

показать полный текст

Итог

my:8181/math.php

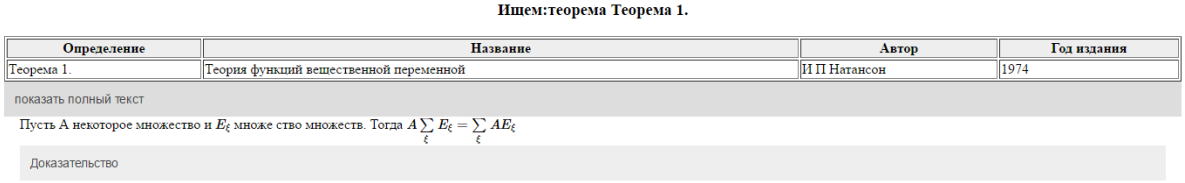
Ищем:определение Уравнение Максвелла

Определение	Название	Автор	Год издания
Уравнение Максвелла	Численные методы в задачах дифракции	Т.Н. Галишникова,А.С. Ильинский	1987

показать полный текст

Уравнениями Максвелла называются уравнения вида$RotH = -ikE\ RotE = ikH, x \in R^3 \backslash \hat{\Omega}$,где Rot-ротор

Рис. 4. Страница вывода: случай одного совпадения



Ищем:теорема Теорема 1.

Определение	Название	Автор	Год издания
Теорема 1.	Теория функций вещественной переменной	И П Натансон	1974

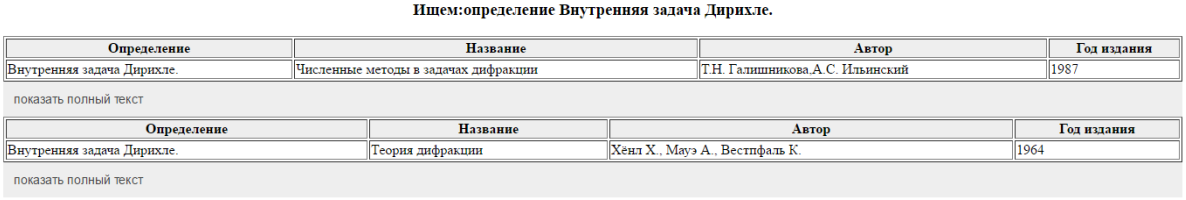
показать полный текст

Пусть A некоторое множество и E_ξ множе ство множеств. Тогда $A \sum\limits_{\xi} E_\xi = \sum\limits_{\xi} AE_\xi$

Доказательство

Рис. 5. Страница вывода: случай большего количества совпадений

В случае более сложных конструкций, таких как теоремы или леммы, необходимо также выводить и доказательство. При нажатии на кнопку «показать полный текст» отображается текст теоремы и кнопка, при нажатии на которую будет возможно открытие текста доказательства.



Ищем:определение Внутренняя задача Дирихле.

Определение	Название	Автор	Год издания
Внутренняя задача Дирихле.	Численные методы в задачах дифракции	Т.Н. Галишникова,А.С. Ильинский	1987

показать полный текст

Определение	Название	Автор	Год издания
Внутренняя задача Дирихле.	Теория дифракции	Хёнл Х., Мауэ А., Вестпфаль К.	1964

показать полный текст

Рис. 6. Страница вывода: случай сложной структуры

В заключение укажем дальнейшие планы по развитию данной работы. Прежде всего, создание средств, позволяющих сохранить семантику при выводе контента, аннотирование терминов и формул.

Работа выполнена за счет средств субсидии, выделенной Казанскому федеральному университету для выполнения государственного задания в сфере научной деятельности, проект 1.2368.2017/ПЧ, и при частичной финансовой поддержке РФФИ и Правительства Республики Татарстан в рамках научного проекта № 15-47-02472.

Литература

1. Гафурова П.О. *Метод обработки математических документов в формате OMDoc* // Тр. Матем. центра им. Н. И. Лобачевского. – Казань: Изд-во Казан. матем. об-ва, 2016. – Т. 53. – С. 70–73.

2. Kohlhase M. *OMDoc: An Open Markup Format for Mathematical Documents [version 1.2]* // Lecture Notes in Artificial Intelligence. – 2006. – V. 4180. – 428 p.

3. Kohlhase M. *Using LaTeX as a Semantic Markup Format*. URL: https://kwarc.info/kohlhase/papers/mcs08-stex.pdf.

4. *KWARC: Knowledge Adaptation and Reasoning for Content*. URL: https://kwarc.info/

5. Kohlhase M., David C., Ginev D., Cornely J. *eMath 3.0: Building Blocks for a Social and Semantic Web for Online Mathematics & eLearning* // Computer Science, Jacobs University Bremen, Germany. – October 27, 2010. – 14 p.

6. Kohlhase M., Iancu M. *Co-Representing Structure and Meaning of Mathematical Documents* // Computer Science, Jacobs University Bremen, Germany. – October 26, 2015. – 24 p.

7. Kohlhase M. *OMDoc: An Open Markup Format for Mathematical Documents* // FB Informatik, Universitat des Saarlandes D-66041 Saarbrucken, Germany. – 2000. – 64 p.

8. Елизаров А.М., Липачев Е.К., Малахальцев М.А. *Веб-технологии для математика: основы MathML. Практическое руководство* // М.: ФИЗМАТЛИТ, 2010. – 192 с.

9. Елизаров А.М., Липачев Е.К., Малахальцев М.А. *Языки разметки семантического веба. Практические аспекты*. – Казань, 2008.

10. Елизаров А. М., Липачев Е. К., Малахальцев М.А. *Основы MATHML. Представление математических текстов в Internet*. – Казань, 2008.

METHOD OF SEMANTIC REPRESENTATION DIGITAL MATHEMATIC DOCUMENTS

P.O. Gafurova

Several works of semantic representation of mathematical documents was reviewed. We also designed the language of semantic representation of mathematical documents, serviced the processing of this language and possibilites for its semantic search and representation of the given language.

Keywords: semantic Web, semantic, OMDoc, semantic representation of mathematics documents.

УДК 519.7; 512.581

О МАСКИРОВКЕ АЛГЕБРАИЧЕСКИХ ПЛАТФОРМ В КРИПТОГРАФИИ С ОТКРЫТЫМ КЛЮЧОМ

К.И. Емельянов[1]

1 *kirillemelyanov11041995@gmail.com*; Казанский (Приволжский) федеральный университет, Институт математики и механики им. Н.И. Лобачевского

В статье обсуждается маскировка алгебраических платформ, таких как группы и группоиды. Идея подобной маскировка переносится на более сложную платформу – 2-категорию.

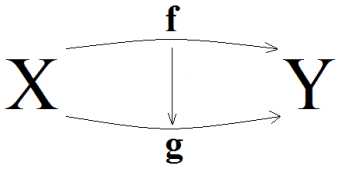
Ключевые слова: криптография, маскировка алгебраических платформ, 2-категория.

В работе [1] был предложен метод маскировки алгебраических платформ, позволяющий при некоторых предположениях гарантировать невзламываемость криптографических протоколов в течение любого наперед заданного времени. В работе [2] были описаны некоторые приложения этого метода.

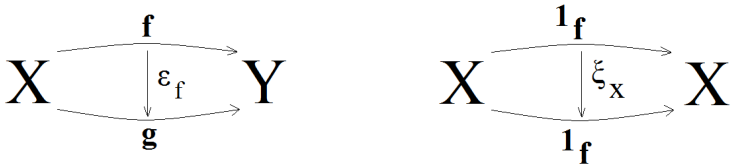
Смысл маскировки в том, что прежде чем противник сможет атаковать криптографический протокол, он должен будет найти некий маскирующий элемент c. Но для этого ему понадобится время, которое можно сделать любым наперед заданным. В группе G можно ввести маскирующий элемент $c \in G$, который будет заменять определённую в группе операцию умножения. Например, это можно сделать таким образом: $a * b = acb$. В результате получается группа $G(c)$ с новой единицей c^{-1}: $a^{-1} = c^{-1}a^{-1}c^{-1}$. Очевидно, эту группу также можно маскировать. Отметим, что $G \cong G(c)$.

В [1] показано, как аналогичным способом можно маскировать группоиды, то есть категории, в которых каждый морфизм обратим. Оказалось также, что похожая конструкция позволяет указать общий способ построения произвольных группоидов. Наша цель в данной работе — описать метод маскировки для принципиально новой для криптографии алгебраической платформы — 2-категорий.

Напомним, что такое 2-категория (см. [3], [4]). Пусть K — категория с объектами X, Y, Z, ... и морфизмами f, g, h, ... (1-морфизмы). Пусть для каждой пары X, Y множество морфизмов $K(X, Y)$ само является категорией, объекты которой — 1-морфизмы. Морфизмы этой категории (морфизмы между 1-морфизмами) будут называться 2-морфизмами и обозначаться так:



Для 2-морфизмов определены два вида суперпозиций, вертикальные и горизонтальные. Горизонтальные суперпозиции будем обозначать так: $\alpha_2 \circ \alpha_1$. Относительно каждой суперпозиции существуют единицы. Обозначим вертикальную единицу через ε_f, а горизонтальную — через ξ_x. Графически их можно изобразить так:

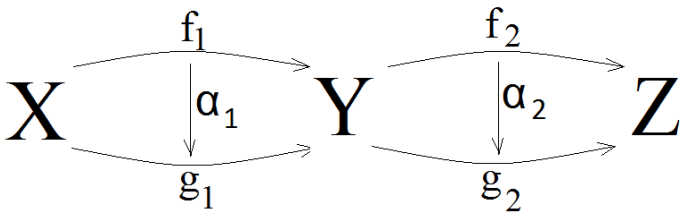


Можно замаскировать вертикальную, горизонтальную или обе композиции одновременно. Замаскируем, например, горизонтальную композицию.

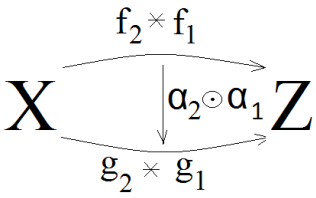
Для каждого объекта Y (1-категории) выбирается маскирующий *обратимый* 1-морфизм $c_Y : Y \to Y$. Это даст маскировку в 1-категории K: вместо суперпозиции gf появляется $g * f = gc_Y f$. Графически:

$$X \xrightarrow{f} Y \xrightarrow{c_Y} Y \xrightarrow{g} Z$$

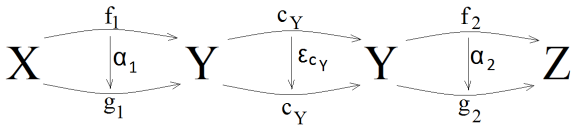
Определим новую горизонтальную суперпозицию 2-морфизмов α_1 и α_2:



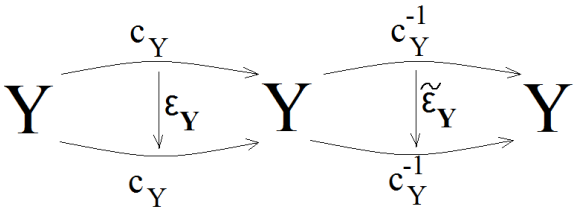
Результат должен иметь вид:



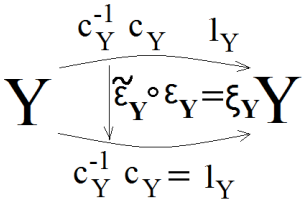
Точное определение: $\alpha_2 \odot \alpha_1 = \alpha_2 \circ \varepsilon_Y \circ \alpha_1$.



Через ε_Y здесь обозначена вертикальная единица ε_{c_Y} Необходимо потребовать обратимость каждого ϵ_Y относительно горизонтальной композиции. То есть должны существовать 2-морфизмы $\tilde{\varepsilon}_Y$



такие, что $\tilde{\varepsilon}_Y \circ \varepsilon_Y = \xi_Y$, $\varepsilon_Y \circ \tilde{\varepsilon}_Y = \xi_Y$:



Так как в $K_{(c)}$ как 1-категории единичные 1-морфизмы – это c_Y^{-1}, то в замаскированной 2-категории горизонтальные единицы – это $\tilde{\varepsilon}_Y$.

Вертикальная суперпозиция останется той же самой. В результате получаем новую (замаскированную) 2-категорию $K_{(c)}$, эквивалентную исходной. Но без знания маскирующих морфизмов вычисления в ней оказываются невозможными. В

дальнейшем эта конструкция будет, как и в [1], [2], использована для обеспечения криптостойкости криптографических протоколов.

Литература

1. Gaynullina, A. R., Tronin S. N. *Some New Platforms for Algebraic Cryptography and One Method of Increasing the Security* // Lobachevskii Journal of Mathematics. – 2016. – V. 37. – No. 6. – P. 768–776.

2. Емельянов К. И. *Использование групп матриц и соответствующих им категорных группоидов для конструирования криптографических протоколов* – Бакалаврская выпускная работа. – Казань, 2016.

3. Маклейн С. *Категории для работающего математика.* – М.: ФИЗМАТЛИТ, 2004. – 352 с.

4. Кондратьев Г. В. *Категории и некоторые их приложения.* – М.: ИНФРА-М, 2017. – 174 с.

ON THE MASKING OF ALGEBRAIC PLATFORMS IN PUBLIC KEY CRYPTOGRAPHY

K.I. Emelyanov

The paper discusses the masking of algebraic platforms, such as groups and groupoids. The idea of such a masking is transferred to a more complex platform — a 2-category.

Keywords: cryptography, masking of an algebraic platform, 2-category.

УДК 532.5.013.12

О РОЛИ НАСЛЕДСТВЕННОЙ СОСТАВЛЯЮЩЕЙ ГИДРОДИНАМИЧЕСКОЙ СИЛЫ ПРИ ДВИЖЕНИИ СФЕРИЧЕСКОГО ВИБРОРОБОТА В ВЯЗКОЙ ЖИДКОСТИ

О.С. Жучкова[1], А.Н. Нуриев[2]

1 *oszaharova@kpfu.ru*; Казанский (Приволжский) федеральный университет, Институт математики и механики им. Н.И. Лобачевского

2 *corei7tesla3@gmail.com*; Казанский (Приволжский) федеральный университет, Институт математики и механики им. Н.И. Лобачевского

В работе проводится исследование вопросов о структуре гидродинамической силы сопротивления, возникающей при периодическом движении сферического виброробота в жидкости, и влиянии различных ее составляющих на процесс и эффективность движения. В том числе, выявляется роль наследственной силы сопротивления в динамике движения робота. Иследование проводится в рамках прямого численного моделирования с использованием программного пакета OpenFoam. Показано, что наследственная составляющая силы в случае конечных периодов движения дает вклад в суммарную силу, сравнимый с квазистационарным. Ее влияние существенно снижает эффективность рассматриваемого механизма движения для случая высокочастотных колебаний.

Ключевые слова: виброробот, гидродинамическое сопротивление, вязкая жидкость, самодвижущееся устройство, наследственные силы, силы присоединенных масс, квазистационарные силы.

Определение гидродинамических сил, возникающих при движении сферического тела в жидкости, относится к классическим проблемам гидромеханики. В данной работе она рассматривается применительно к задаче о поступательном дви-

жении сферического виброробота – самодвижущегося устройства, состоящего из твердого герметичного сферического корпуса, помещенного в вязкую жидкость, и подвижной внутренней массы, совершающей периодические колебания внутри него. Возможность направленного движения такой системы обеспечивает нелинейное сопротивление жидкости. Вопросы о структуре, величине ее составляющих и их влиянии на движении виброробота рассматриваются в настоящей работе.

Современные модели гидродинамических сил (см., напр. [1]), описывающих воздействие вязкой жидкости на сферу при нестационарном поступательном движении, основываются (как и в случае малых чисел Рейнольдса [2]) на выделении трех основых эффектов: квазистационарного сопротивления (F_{st}),сил присоединенных масс (F_a) и сил наследственного сопротивления (F_h):

$$F = F_{st} + F_a + F_h. \tag{1}$$

Теоретическая модель, исследующая возможности движения виброробота за счет квазистационарного сопротивления, была представлена в работе [3]. При таких условиях эффективность движения системы в диапазоне чисел Рейнольдса $Re_{av} \leq 10^3$ могла бы достигать 7.9% (где Re_{av} – число Рейнольдса, вычисленное по средней скорости движения). Оптимальными для этого случая являются двухфазные периодические законы движения внутренней массы, где длинные фазы медленного поступательного движения, на которых сфера испытывает малое сопротивление, сменяются короткими фазами быстрого возвратного движения, позволяющими за счет высокого сопротивления с минимальным откатом корпуса вернуть внутренний груз в начальное положение. Именно эти результаты были выбраны в качестве отправной точки в настоящей работе. С использованием методов численного моделирования было рассмотрено движение виброробота по подобным двухфазным законам в диапазоне относительно небольших значений числа Рейнольдса $Re_{av} \leq 102$. Фрагмент закона движения u_M с периодом $\tau = 1$ изображен на рис 1.

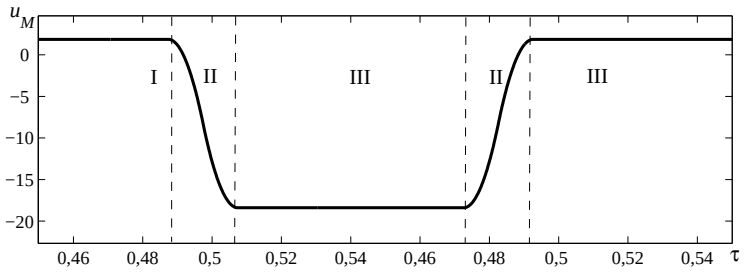


Рис. 1. Фрагмент периодического закона движения корпуса $u_M(\tau)$

При расчете гидродинамического взаимодействия проводились решение полной системы уравнений Навье-Стокса (на основе численной модели [4]) и покомпонентная оценка составляющих сопротивления для каждого моделируемого случая в соответствии с (1). Было показано, что сила на двух отрезках ускорения (см. области II на рис. 1) практически полностью определяется силой присоединенных масс пропорциональной ускорению. Коэффициент присоединенных масс при этом является константой $C_a = 0.5$, что согласуется с результатами многих исследований, проведенных для сферы [5]. Таким образом, суммарный вклад сил на отрезках ускорения

в рамках полного периода движения приблизительно равен нулю, а, следовательно, направленное движение виброробота является результатом сил, действующих на прямой и возвратной фазах движения (см. области I, III на рис. 1). На обеих фазах согласно представлению (1) в отсутствие ускорения сила определяется наследственной и квастационарной составляющими, коэффициенты этих сил на фазах определяются следующими формулами:

$$C_D^+ = C_h^+ + C_{st}^+ = \frac{\langle F \rangle_+}{u_+^2}, \quad C_D^- = C_h^- + C_{st}^- = \frac{\langle F \rangle_-}{u_-^2}.$$

Здесь треугольными скобками с индексом “+” или “–” обозначено осреднение сил на прямой и возвратной фазе соответственно. На рис. 2 представлены результаты расчетов, выполненных при фиксированной средней скорости Re_{av} и периоде движения κ с переменной относительной продолжительностью фаз b. Изменение b напрямую влияет на скорости движения на фазах u_+, u_-, по которым вычисляются мгновенные числа Рейнольдса Re_+ и Re_- соответственно. Вклад от квазистационарной составляющей в среднюю силу в зависимости от мгновенного числа Рейнольдса представлен на графике сплошной линией.

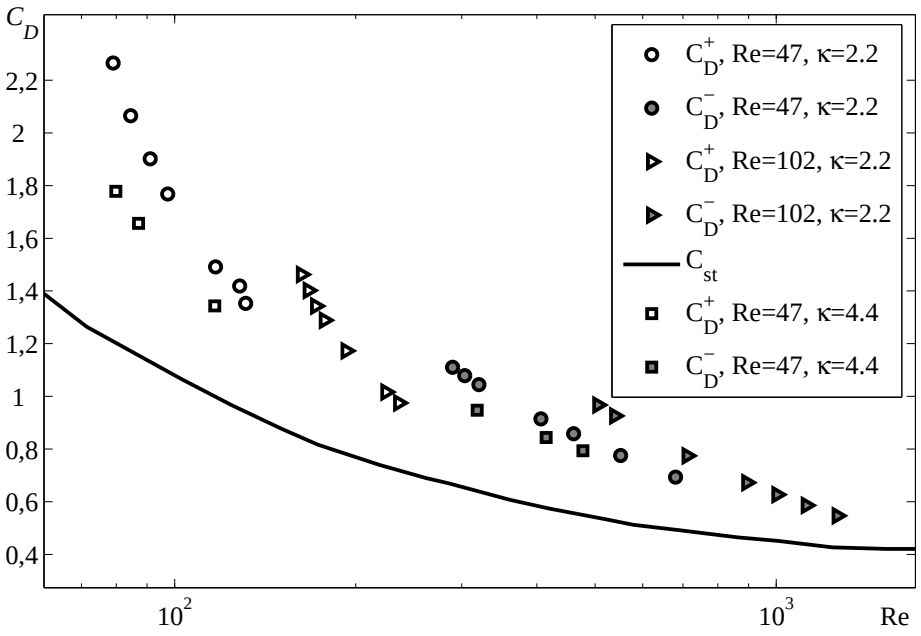


Рис. 2. Результаты измерений осредненных значений коэффициента силы на прямой и возвратной фазах для различных b

Как видно наследственная составляющая силы в случае конечных периодов движения дает вклад в суммарную силу, сравнимый с квазистационарным. Ее влияние существенно снижает эффективность рассматриваемого механизма движения для случая высокочастотных колебаний по сравнению с предельными оценками квазистационарной модели [3].

Работа выполнена при финансовой поддержке РФФИ (проект 16-31-00462).

Литература

1. Mei R. *Velocity fidelity of flow tracer particles* // Experiments in Fluids. –1996. – V. 22. – № 13.

2. Basset A.B. *A Treatise on Hydrodynamics*, V. 2. – Dover, 1888.

3. Егоров А.Г., Захарова О.С. *Оптимальное квазистационарное движение виброробота в вязкой жидкости* // Изв. вузов. Матем. – 2012. – № 2. – С. 57–64.

4. Нуриев А.Н., Зайцева О.Н. *Решение задачи об осциллирующем движении цилиндра в вязкой жидкости в пакете OpenFOAM* // Вестн. Казанск. технол. ун-та. – 2013. – Т. 16. – № 8. – С. 116-123.

5. Chang E.J., Maxey, M.R. *Unsteady flow about a sphere at low to moderate Reynolds number. Part 2. Accelerated motion* // J. Fluid Mech. – 1995. – V. 303. – P. 133–153.

ABOUT THE ROLE OF THE HISTORY COMPONENT OF THE HYDRODYNAMIC FORCE DURING THE MOTION OF A SPHERICAL VIBRATION-DRIVEN ROBOT IN A VISCOUS FLUID

O.S. Zhuchkova, A.N. Nuriev

The paper studies the problems of the structure of the hydrodynamic drag force that arises during the periodic motion of a spherical vibration-driven robot in a fluid and the influence of its various components on the process and efficiency of motion. In particular, the role of the history force of resistance in the movement dynamics of the robot is revealed. The research is carried out in the framework of direct numerical simulation using the OpenFoam software package. It is shown that the history component of the force in the case of finite periods of motion contributes to the total force comparable to the quasistationary force. Its influence significantly reduces the efficiency of the considered motion mechanism for the case of high-frequency oscillations.

Keywords: vibration-driven robot, hydrodynamic resistance, viscous fluid, self-propulsion device, history force, added-mass force, quasistationary force.

УДК 517.95

ОБ УСТОЙЧИВОСТИ РЕШЕНИЯ ОДНОЙ НЕЛОКАЛЬНОЙ ЗАДАЧИ ДЛЯ ГИПЕРБОЛИЧЕСКОГО УРАВНЕНИЯ С СИНГУЛЯРНЫМ КОЭФФИЦИЕНТОМ

Н.В. Зайцева[1]

1 *n.v.zaiceva@yandex.ru*; Казанский (Приволжский) федеральный университет, Институт математики и механики им. Н.И. Лобачевского

В работе для гиперболического уравнения с сингулярным коэффициентом поставлена нелокальная задача в прямоугольной области. Методом спектрального анализа доказаны теоремы единственности, существования и устойчивости решения задачи. Решение построено в виде ряда Фурье-Бесселя, и приведено обоснование сходимости ряда в классе регулярных решений.

Ключевые слова: нелокальная задача, гиперболическое уравнение, сингулярный коэффициент, ряд Фурье-Бесселя, устойчивость.

Рассмотрим в прямоугольной области $D = \{(x,t)|0 < x < l, 0 < t < T\}$, $l, T > 0$, координатной плоскости Oxt гиперболическое уравнение вида

$$\Box_B u(x,t) \equiv u_{tt} - u_{xx} - \frac{k}{x} u_x = 0,$$

где $k \geq 1$ – заданное действительное число.

Постановка задачи. Найти функцию $u(x,t)$, удовлетворяющую условиям:

$$u(x,t) \in C^1(\overline{D}) \cap C^2(D), \tag{1}$$

$$\Box_B u(x,t) \equiv 0, \qquad (x,t) \in D, \tag{2}$$

$$u(x,0) = \varphi(x), \qquad u_t(x,0) = \psi(x), \qquad 0 \leq x \leq l, \tag{3}$$

$$\int_0^l u(x,t)\, x^k\, dx = A = \text{const}, \qquad 0 \leq t \leq T, \tag{4}$$

где A – заданное число, $\varphi(x)$, $\psi(x)$ – заданные достаточно гладкие функции, удовлетворяющие условиям согласования

$$\int_0^l \varphi(x)\, x^k\, dx = A, \qquad \int_0^l \psi(x)\, x^k\, dx = 0. \tag{5}$$

Нелокальная задача (1) – (4) сведена к эквивалентной задаче (1) – (3) с локальным граничным условием

$$u_x(l,t) = 0, \qquad 0 \leq t \leq T. \tag{6}$$

Методом спектрального анализа [1, 2] решение задачи (1) – (3), (6) получено в виде суммы ряда Фурье-Бесселя

$$u(x,t) = \sum_{n=1}^{\infty} u_n(t) X_n(x), \tag{7}$$

где

$$u_n(t) = \varphi_n \cos\lambda_n t + \frac{\psi_n}{\lambda_n} \sin\lambda_n t, \tag{8}$$

$$\varphi_n = \int_0^l \varphi(x) x^k X_n(x)\, dx, \quad \psi_n = \int_0^l \psi(x) x^k X_n(x)\, dx,$$

$$X_n(x) = \frac{1}{||\widetilde{X}_n||_{L_{2,\rho}(0,l)}} \widetilde{X}_n(x),$$

$$\widetilde{X}_n(x) = x^{\frac{1-k}{2}} J_{\frac{k-1}{2}}(\lambda_n x), \quad n \in \mathbb{N},$$

$$||\widetilde{X}_n||^2_{L_{2,\rho}(0,l)} = \int_0^l \rho(x)\, \widetilde{X}_n^2(x)\, dx, \quad \rho(x) = x^k.$$

Здесь $J_\nu(z)$ – функция Бесселя первого рода порядка ν. Собственные значения μ_n определяются как нули уравнения

$$J_{\frac{k+1}{2}}(\mu) = 0, \quad \mu = \lambda l.$$

В работе [3] доказаны следующие утверждения

Теорема 1. *Если существует решение задачи* (1) – (3), (6), *то оно единственно.*

Теорема 2. *Если функции* $\varphi(x)$ *и* $\psi(x)$ *удовлетворяют условиям* $\varphi(x) \in C^2[0,l]$, $\psi(x) \in C^1[0,l]$ *и*

$$\varphi'(0) = \varphi''(0) = \psi'(0) = \varphi'(l) = \psi'(l) = 0,$$

то существует единственное решение $u(x,t)$ *задачи* (1) – (3), (6), *определяемое рядом* (7), *при этом* $u(x,t) \in C^2(\overline{D})$.

Теорема 3. *Если функции* $\varphi(x)$ *и* $\psi(x)$ *удовлетворяют условиям* $\varphi(x) \in C^2[0,l]$, $\psi(x) \in C^1[0,l]$,

$$\varphi'(0) = \varphi''(0) = \psi'(0) = \varphi'(l) = \psi'(l) = 0$$

и условиям (5), *то существует единственное решение задачи* (1) – (5), *определяемое рядом* (7), *при этом* $u(x,t) \in C^2(\overline{D})$.

При обосновании устойчивости построенного решения вводится известная норма и доказана

Теорема 4. *Для решения задачи* (1) – (5) *справедлива оценка*

$$||u||_{L_{2,\rho}(0,l)} \le C_1(||\varphi||_{L_{2,\rho}(0,l)} + ||\psi||_{L_{2,\rho}(0,l)}), \tag{10}$$

где

$$||f||^2_{L_{2,\rho}(0,l)} = \int_0^l \rho(x)|f(x)|^2 dx, \;\; \rho(x) = x^k.$$

Доказательство. Исходя из формулы (7) с учетом оценки

$$|u_n(t)| \le C_2\left(|\varphi_n| + \frac{|\psi_n|}{n}\right),$$

которая следует непосредственно из (8), вычислим

$$||u||^2_{L_{2,\rho}(0,l)} = \int_0^l x^k u^2(x,t)\,dx = \int_0^l x^k \sum_{n=1}^{\infty} u_n(t)X_n(x) \sum_{m=1}^{\infty} u_m(t)X_m(x)\,dx =$$

$$= \sum_{m,n=1}^{\infty} u_n(t)u_m(t) \int_0^l x^k X_n(x)X_m(x)\,dx = \sum_{n=1}^{\infty} u_n^2(t) \int_0^l x^k X_n^2(x)\,dx =$$

$$= \sum_{n=1}^{\infty} u_n^2(t) \le 2C_2^2 \sum_{n=1}^{\infty}\left(|\varphi_n|^2 + \frac{1}{n^2}|\psi_n|^2\right) \le 2C_2^2\left(\sum_{n=1}^{\infty}\varphi_n^2 + \sum_{n=1}^{\infty}\psi_n^2\right) =$$

$$= 2C_2^2\left(||\varphi||^2_{L_{2,\rho}(0,l)} + ||\psi||^2_{L_{2,\rho}(0,l)}\right).$$

Отсюда следует справедливость оценки (10). ■

Литература

1. Сабитов К. Б., Вагапова Э. В. *Задача Дирихле для уравнения смешанного типа с двумя линиями вырождения в прямоугольной области* // Дифференц. уравнения. – 2013. – Т. 49. – № 1. – С. 68–78.

2. Сафина Р. М. *Задача Келдыша для уравнения смешанного типа второго рода с оператором Бесселя* // Дифференц. уравнения. – 2015. – Т. 51. – № 10. – С. 1354–1366.

3. Zaitseva N. V. *Keldysh type problem for B-hyperbolic equation with integral boundary value condition of the first kind* // Lobachevskii J. of Math. – 2017. – V. 38. – № 1. – P. 162–169.

STABILITY OF THE SOLUTION OF A NONLOCAL BOUNDARY VALUE PROBLEM FOR A HYPERBOLIC EQUATION WITH SINGULAR COEFFICIENT

N.V. Zaitseva

We consider a nonlocal boundary value problem for a hyperbolic equation with a singular coefficient in a rectangular domain. The existence, uniqueness and stability of the solution of the problem are established by means of the spectral method. The solution of the problem is obtained in an explicit form. As sum of a Fourier-Bessel series; its convergence is proved in the class of regular solutions.

Keywords: nonlocal problem, hyperbolic equation, singular coefficient, Fourier-Bessel series, stability.

УДК 519.7

О НЕКОТОРЫХ СХЕМАХ ЧАСТИЧНЫХ ЗАТЕМНЕННЫХ ПОДПИСЕЙ, ИСПОЛЬЗУЮЩИХ СЛОЖНОСТЬ ЗАДАЧИ О ДИСКРЕТНОМ ЛОГАРИФМЕ

А.И. Зиятдинова[1]

1 *aiziyatdinova@ksu.ru*; Казанский (Приволжский) федеральный университет, Институт математики и механики им. Н. И. Лобачевского

Приведены новые примеры частичных затемненных цифровых подписей, основанных на сложности задачи о дискретном логарифме.

Ключевые слова: затемненные цифровые подписи, частичные затемненные подписи, задача о дискретном логарифме.

Разновидностью затемненных цифровых подписей (или слепых, или подписей вслепую) [1] являются частичные затемненные подписи [2]. Известно довольно много примеров таких подписей, в том числе, основанных на сложности задачи о дискретном логарифме (см., напр., [3]). В нашей работе описываются еще два примера подписей такого типа.

Особенностью частичных затемненных подписей (partially blind signatures) является то, что для подписания вместе с затемненной величиной (это может быть идентификатор электронной банкноты) отправляется открытый параметр, который используется в алгоритме подписания

В статье [4] приводятся примеры подписей, аналогичных цифровой подписи Эль-Гамаля. Авторы представляют некоторые типы подписей, которые наиболее эффективны для клиента – покупателя и подписывающего — банка. Рассмотрим схемы данных подписей.

Даны два открытых больших простых числа p, q, причем $q|p-1$. В поле $\mathbb{Z}_p = \{0,1,2,\ldots,p-1\}$ выбран открытый элемент α порядка q.

Для цифровой подписи выбирается случайное число $s_A \in \mathbb{Z}^*_{p-1}$ и вычисляется $p_A = \alpha^{s_A} \pmod p$. В данном случае s_A — секретный ключ подписывающего, а p_A — открытый ключ. Эти значения остаются постоянными для всех подписываемых сообщений. Чтобы подписать сообщение $m \in \mathbb{Z}_{p-1}$ подписывающий выбирает случайное число $k \in \mathbb{Z}_{p-1}$, вычисляет $r = \alpha^k \pmod p$ и решает уравнение

$$s \equiv s_A(m+r) - k \pmod{(p-1)} \qquad (*)$$

относительно параметра s. Тройка $(m; r, s)$ — подписанное сообщение. Правильность подписи можно осуществить, проверив равенство

$$r\alpha^s \equiv p_A^{m+r} \pmod p.$$

Далее авторы [4] представляют некоторые другие варианты схемы цифровых подписей Мета-Эль-Гамаль, которые так же эффективны, как и схема, рассмотренная выше. Чтобы подписать сообщение, клиент вычисляет уравнение, а банк проверяет справедливость соответствующего сравнения, представленного в следующем списке:

(1) $s = (m+r)s_A + k;\ \alpha^s \equiv p_A^{m+r} r$,
(2) $s = s_A + k(m+r);\ \alpha^s \equiv p_A r^{m+r}$,
(3) $s = s_A(m+r) + k - m;\ \alpha^{m+s} \equiv p_A^{m+r} r$,
(4) $s = s_A + k(m+r) - m;\ \alpha^{m+s} \equiv p_A r^{m+r}$,
(5) $s = s = s_A(m+r) + k - r;\ \alpha^{r+s} \equiv p_A^{m+r} r$,
(6) $s = s_A + k(m+r) - r;\ \alpha^{r+s} \equiv p_A r^{m+r}$.

Рассмотрим затемненную версию цифровой подписи $(*)$. В этом случае имеются три участника протокола, из которых для нас важны только два: Банк, который подписывает, и Клиент (Алиса), который снимает деньги со счета и для этого посылает Банку затемненный идентификатор m. Когда Банк подпишет этот идентификатор, Клиент убирает затемнение и получает электронную банкноту (e-cash).

Распишем подробно схему.

1) Банк (подписывающий) генерирует случайное число $\widetilde{k} \in \mathbb{Z}_q$, вычисляет $\widetilde{r} \equiv \alpha^{\widetilde{k}} \pmod p$ и отправляет $\widetilde{r}$ клиенту.

2) Клиент в свою очередь выбирает случайные числа $a, b \in \mathbb{Z}_q$ и вычисляет $r = \widetilde{r}^a \alpha^b \pmod p$ и $\widetilde{m} = a^{-1}(m+r) - \widetilde{r} \pmod q$. Вычисленное $\widetilde{m}$ отправляется банку.

3) Банк подписывает затемненное сообщение $\widetilde{m}$, вычисляя $\widetilde{s} = s_N(\widetilde{m} + \widetilde{r}) - \widetilde{k} \pmod q$. Затем $\widetilde{s}$ отправляется клиенту.

4) Клиент вычисляет $s = a\widetilde{s} - b \pmod q$

Подписанным сообщением (электронной банкнотой) является тройка $(m; r, s)$.

Для того чтобы узнать, верна ли подпись, нужно проверить следующее сравнение: $\alpha^s r \equiv p_N^{m+r} \pmod p$, или $\alpha^s \equiv p_N^{m+r} r^{-1} \pmod p$.

Далее будут рассматриваться подписи (1) и (3) из списка, представленного выше. Поэтому представим их затемненные варианты, которые предлагаются в [4]:

$$(1)\quad \widetilde{m} = a^{-1}(m+r) - \widetilde{r}, \quad s = a\widetilde{s} + b;$$
$$(3)\quad \widetilde{m} = a^{-1}(m+r) - \widetilde{r}, \quad s = a(\widetilde{m} + \widetilde{s}) + b - m.$$

Проверочные равенства остаются теми же, как и в соответствующих незатемненных вариантах: в случае (1): $\alpha^s \equiv p_N^{m+r} r$, в случае (3): $\alpha^{s+m} \equiv p_N^{m+r} r$, или $\alpha^s \equiv p_N^{m+r} r\alpha^{-m}$.

В процессе проверки подписей, выявились неточности в работе [4]. Поэтому нам пришлось несколько видоизменить некоторые данные в этих двух вариантах подписей. Во-первых, в обоих случаях изменится r, вычисляемое клиентом. Оно будет иметь вид: $r = \widetilde{r}^{-a}\alpha^b$. Во-вторых, в варианте (3) изменится незатемненная подпись, которую вычисляет клиент: $s = a(\widetilde{m} + \widetilde{s} + \widetilde{r}) + b - 2m - r$.

Подтвердим, что теперь проверочные сравнения будут верными. Для варианта (1):

$$\alpha^s = \alpha^{a\widetilde{s}+b} = \alpha^{as_N(\widetilde{m}+\widetilde{r})t - a\widetilde{k}+b} = \alpha^{as_N(a^{-1}(m+r)-\widetilde{r}+\widetilde{r})}\alpha^{-a\widetilde{k}+b} = \alpha^{s_N(m+r)} r = p_N^{m+r} r.$$

Для варианта (3):

$$\alpha^s = \alpha^{a(\widetilde{m}+\widetilde{s}+\widetilde{r})+b-2m-r} = \alpha^{a(a^{-1}(m+r)-\widetilde{r}+s_N(a^{-1}(m+r)-\widetilde{r}+\widetilde{r})-\widetilde{k}+\widetilde{r})+b-2m-r} =$$
$$\alpha^{s_N(m+r)}\alpha^{-a\widetilde{k}+b}\alpha^{m+r-2m+r} = p_N^{m+r} r\alpha^{-m}$$

Проверки выполняются, следовательно, можно сделать вывод, что внесенные изменения верны.

Далее попытаемся ввести параметр t в подписи (1) и (3). Этот параметр может иметь разный смысл. В отличие от [1], мы будем предполагать, что это сумма, которую Клиент желает снять со счета. Разберем отдельно каждый вариант. Для начала рассмотрим подпись (1): $\widetilde{s} = s_N(\widetilde{m} + \widetilde{r})t - \widetilde{k}$.

1) Банк генерирует случайное число $\widetilde{k} \in \mathbb{Z}_q$, вычисляет $\widetilde{r} \equiv \alpha^{\widetilde{k}} \pmod{p}$ и отправляет $\widetilde{r}$ Клиенту.

2) Клиент в свою очередь выбирает случайные числа $a, b \in \mathbb{Z}_q$ и вычисляет $r = \widetilde{r}^{-a}\alpha^b \pmod{p}$ и $\widetilde{m} = a^{-1}(m+r) - \widetilde{r} \pmod{q}$. Вычисленное $\widetilde{m}$ и параметр – сумма t отправляются банку.

3) Банк подписывает затемненное сообщение $\widetilde{m}$, вычисляя $\widetilde{s} = s_N(\widetilde{m} + \widetilde{r})t - \widetilde{k} \pmod{q}$. Затем $\widetilde{s}$ отправляется клиенту.

4) Клиент вычисляет $s = a\widetilde{s} + b \pmod{q}$

Проверим, выполняется ли соотношение проверки:

$\alpha^s = \alpha^{a\widetilde{s}+b} = \alpha^{as_N(\widetilde{m}+\widetilde{r})t - a\widetilde{k}+b} = \alpha^{as_N(a^{-1}(m+r)-\widetilde{r}+\widetilde{r})t}\alpha^{-a\widetilde{k}+b} = \alpha^{s_N(m+r)t} r = p_N^{(m+r)t} r.$

Проверка выполнена успешно. Следовательно, ввод параметра возможен.

Аналогично вводим параметр t в подпись (3): $\widetilde{s} = s_N(\widetilde{m} + \widetilde{r})t - \widetilde{k}$. Схема подписи будет та же, поэтому сразу рассмотрим проверочное равенство:

$\alpha^s = \alpha^{a(\widetilde{m}+\widetilde{s}+\widetilde{r})+b-2m-r} = \alpha^{a(a^{-1}(m+r)-\widetilde{r}+s_N(a^{-1}(m+r)-\widetilde{r}+\widetilde{r})t-\widetilde{k}+\widetilde{r})+b-2m-r} = \alpha^{s_N(m+r)t}\alpha^{-a\widetilde{k}+b}\alpha^{m+r-2m+r} = p_N^{(m+r)t} r\alpha^{-m}$

Делаем вывод, что возможность введения параметра подтверждена.

Далее делается проверка того, что Клиент не сможет изменить параметр t (например, увеличить), так как в этом случае проверка подписи уже не выполняется. Изменить подпись Клиент тоже не сможет.

Литература

1. Епишкина А. В., Шимкив М. Я.*Обзор и анализ криптографических схем, реализующих электронную подпись «вслепую»* // Безопасность инф. техн. – 2015. – № 3. – С.51–58.

2. Abe M., Fujisaki E. *How to date blind signatures* // Advances in Cryptology. – AisaCrypt'96, Springer-Verlag, 1996, LNCS 1163. – P. 244–251.

3. Huang Zheng, Chen Ke-fei, Kou Wei-dong. *Untraceable partially blind signature based on DLOG problem* // J. of Zhejiang Univ. SCIENCE. – 2004. – V. 5. – No. 1. – P. 40– 44.

4. Horster P. Michels M., Petersen H. *Efficient blind signature schemes based on the discrete logarithm problem* // Univ. of Technol. Chemiitz-Zwickau, Techn. Report TR-94-6-D. – 1994. – 5 p.

ON SOME SCHEMES OF PARTIALLY BLIND SIGNATURES USING THE COMPLEXITY OF THE DISCRETE LOGARITHM PROBLEM

A.I. Ziyatdinova

The paper describes new examples of partially blind digital signatures based on the complexity of the discrete logarithm problem.

Keywords: programming contests, informatics olympiads, combinatorial tasks.

УДК 372.851

РАЗРАБОТКА МАТЕМАТИЧЕСКИХ ЗАДАНИЙ ДЛЯ СТУДЕНТОВ ИНЖЕНЕРНЫХ НАПРАВЛЕНИЙ В LMS MOODLE

Т.В. Зыкова[1]

1 *zykovatv@mail.ru*; Сибирский федеральный университет, Институт космических и информационных технологий

В работе приводится описание применения редактора формул WIRIS для создания математических заданий в LMS Moodle для электронного обучающего курса по математическому алазизу. Курс создан в рамках модели электронного обучения для студентов инженерных направлений Института космических и информационных технологий Сибирского федерального университета.

Ключевые слова: информационно-коммуникационные технологии, математическая компетентность, электронные обучающие курсы, электронное обучение, LMS Moodle, WIRIS.

В настоящее время в мировых стандартах инженерного образования происходят изменения, связанные с применением информационно-коммуникационных технологий в обучении, современный уровень развития которых открывает большие возможности их использования. В нашей стране требования ФГОС ВО также

предполагают использование интерактивных форм обучения. Сочетание традиционных форм лекционных и практических занятий с самостоятельной домашней работой в онлайн-режиме с использованием личностно ориентированной веб-среды способствует более глубокому усвоению материала. Работа с электронным обучающим курсом позволяет студенту формировать компетенции и оценивать свои знания как на аудиторных занятиях, так и в рамках самостоятельной работы в любое удобное для него время за счет средств удаленного доступа, а преподавателю – осуществлять мониторинг такой учебно-познавательной деятельности [1].

В 2010 г. в Институте космических и информационных технологий СФУ стартовал проект по созданию образовательной среды обучения на базе LMS Moodle, европейской системы дистанционного обучения (Learning Management System – LMS). На платформе данной системы были созданы электронные обучающие курсы (ЭОК) для студентов. Трудности при создании таких курсов создает отсутствие универсальной технологии их разработки, в частности, это касается выбора дидактических материалов. Обучение студентов происходит в сочетании традиционных форм лекционных и практических занятий с самостоятельной домашней работой в онлайн-режиме с использованием личностно ориентированной веб-программы. Контрольные тестирования проводятся в LMS Moodle. Материалы каждого курса представлены модулями, соответствующими изучаемой теме математической дисциплины.

Большим недостатком встроенных в Moodle сервисов по созданию математических заданий является отсутствие вариативности, то есть преподавателю постоянно приходится их обновлять. Подобных проблем можно избежать, используя редактор WIRIS, который может быть интегрирован с LMS Moodle. WIRIS editor — это редактор формул (также называемый редактором уравнений), который полностью написан на языках HTML4 и JavaScript и благодаря этому поддерживается мобильными устройствами. Он совместим с веб-страницами на основе HTML5 и позволяет программировать задания, получить их вариативность, а также полноценную графическую визуализацию. Сама система редактора WIRIS предполагает, что для программирования каждой задачи всегда используется масса настроек: вид ответа (тест, формула, число), вид сравнения эталонного ответа с введенным (равенство, эквивалентность, литературное равенство) и т. д. Возможны дополнительные настройки, например, упрощение или разложение на множители введенного ответа для сравнения с эталонным. Каждую задачу необходимо алгоритмизировать и запрограммировать. Таким образом достигается вариативность задач. Более подробный пример применения WIRIS можно рассмотреть в работе [2].

Интеграция LMS Moodle с редактором WIRIS открывает ряд дополнительных возможностей, которые могут сделать электронный обучающий курс наиболее содержательным, включающим задания не только тестового типа. Поэтому в ближайшей перспективе становится актуальной задача создания банка математических заданий, запрограммированных в редакторе WIRIS.

Исследование выполнено при финансовой поддержке гранта Российского научного фонда (проект № 16–18–10304).

Литература

1. Шершнева В.А. *Формирование математической компетентности студентов инженерного вуза на основе полипарадигмального подхода*: монография. – Красноярск: Изд-во Сиб. гос. аэрокосмич. ун-та им. акад. М. Ф. Решетнёва, 2011. – 268 с.

2. Зыкова Т.В., Кацунова А.С., Цибульский Г.М., Сидорова Т.В., Шершнева В.А. *Математические задания для студентов инженерных направлений в LMS Moodle* // Вестник Красноярск. гос. пед. ун-та им. В.П. Астафьева. – 2016. – № 3 (37). – С. 61–64.

DEVELOPMENT OF MATHEMATICAL TASKS
FOR STUDENTS OF ENGINEERING IN THE LMS MOODLE

T.V. Zykova

The paper provides a description of the use of the equation editor WIRIS for creation of mathematical tasks in the LMS Moodle for electronic training course on mathematical analysis. The course is designed in the framework of model e-learning for students of Engineering Institute of Space and Information technology of the Siberian Federal University.

Keywords: information and communication technology, mathematical competence, e-learning courses, e-learning, LMS Moodle, WIRIS.

УДК 517.956.25

СУЩЕСТВОВАНИЕ ЭНТРОПИЙНЫХ РЕШЕНИЙ АНИЗОТРОПНЫХ ЭЛЛИПТИЧЕСКИХ УРАВНЕНИЙ С ПЕРЕМЕННЫМИ ПОКАЗАТЕЛЯМИ НЕЛИНЕЙНОСТЕЙ В $\mathbb{R}^N$

А.Ш. Камалетдинов[1], Л.М. Кожевникова[2]

1 *kamaletdinovaleksandr@mail.ru*; Стерлитамакский филиал Башкирского государственного университета, факультет математики и информационных технологий

2 *kosul@mail.ru*; Стерлитамакский филиал Башкирского государственного университета, факультет математики и информационных технологий

В пространстве $\mathbb{R}^n$ рассматривается некоторый класс анизотропных эллиптических уравнений с переменными показателями нелинейностей и L_1–правой частью. Доказано существование энтропийных решений в анизотропных пространствах Соболева с переменными показателями. Установлено, что построенное энтропийное решение является ренормализованным решением рассматриваемой задачи.

Ключевые слова: анизотропное эллиптическое уравнение, переменный показатель нелинейности, энтропийное решение, ренормализованное решение.

Для эллиптических уравнений со степенными нелинейностями и L_1-правой частью в работе [1] было предложено понятие энтропийного решения задачи Дирихле и доказаны его существование и единственность. В настоящей работе доказано существование энтропийных решений в пространстве $\mathbb{R}^n = \{\mathrm{x} = (x_1, x_2, \ldots, x_n)\}$, $n \geq 2$, для некоторого класса эллиптических уравнений с переменными показателями нелинейностей

$$\sum_{i=1}^{n} (a_i(\mathrm{x}, u, \nabla u))_{x_i} - |u|^{p_0(\mathrm{x})-2} u - b(\mathrm{x}, u, \nabla u) = f(\mathrm{x}), \quad \mathrm{x} \in \mathbb{R}^n, \tag{1}$$

с функцией $f(\mathrm{x}) \in L_1(\mathbb{R}^n)$.

Обозначим

$$C^+(\mathbb{R}^n) = \{p(\mathrm{x}) \in C(\mathbb{R}^n) : 1 < p^- \le p^+ < +\infty\},$$

где $p^- = \inf\limits_{\mathbb{R}^n} p(\mathrm{x})$, $p^+ = \sup\limits_{\mathbb{R}^n} p(\mathrm{x})$. Приведем условия на функции, входящие в уравнение (1). Пусть $\vec{\mathbf{p}}(\mathrm{x}) = (p_0(\mathrm{x}), p_1(\mathrm{x}), ..., p_n(\mathrm{x})) \in (C^+(\mathbb{R}^n))^{n+1}$. Положим $p_+(\mathrm{x}) = \max_{i=\overline{1,n}} p_i(\mathrm{x})$,

$$\overline{p}(\mathrm{x}) = n\left(\sum_{i=1}^{n} 1/p_i(\mathrm{x})\right)^{-1}, \quad p_*(\mathrm{x}) = \begin{cases} \frac{n\overline{p}(\mathrm{x})}{n-\overline{p}(\mathrm{x})}, & \overline{p}(\mathrm{x}) < n, \\ +\infty, & \overline{p}(\mathrm{x}) \ge n \end{cases}.$$

Будем считать, что

$$p_+(\mathrm{x}) \le p_0(\mathrm{x}) < p_*(\mathrm{x}), \quad \mathrm{x} \in \mathbb{R}^n. \tag{2}$$

Введем обозначения: $\mathrm{a}(\mathrm{x}, s_0, \mathrm{s}) = (a_1(\mathrm{x}, s_0, \mathrm{s}), \ldots, a_n(\mathrm{x}, s_0, \mathrm{s}))$, $\mathrm{s} \cdot \mathrm{t} = \sum\limits_{i=1}^{n} s_i t_i$, $\mathrm{s} = (s_1, \ldots, s_n)$, $\mathrm{t} = (t_1, \ldots, t_n) \in \mathbb{R}^n$, $\mathrm{P}(\mathrm{s}) = \sum\limits_{i=1}^{n} |s_i|^{p_i(\mathrm{x})}$.

Предполагается, что функции $a_i(\mathrm{x}, s_0, \mathrm{s})$, $i = 1, \ldots, n$, $b(\mathrm{x}, s_0, \mathrm{s})$, $\mathrm{x} \in \mathbb{R}^n$, $s_0 \in \mathbb{R}$, $\mathrm{s} \in \mathbb{R}^n$ каратеодориевы. Пусть существуют неотрицательные функции $\Phi_i(\mathrm{x}) \in L_{p_i'(\cdot)}(\mathbb{R}^n)$, $p_i'(\mathrm{x}) = p_i(\mathrm{x})/(p_i(\mathrm{x})-1)$, $i = 1, \ldots, n$, $\Phi_0(\mathrm{x}) \in L_1(\mathbb{R}^n)$, непрерывные неубывающие функции $\widehat{a}_i : \mathbb{R}^+ \to \mathbb{R}^+$, $i = 1, \ldots, n$, $\widehat{b} : \mathbb{R}^+ \to \mathbb{R}^+$, положительное число $\overline{a}$ такие, что при п.в. $\mathrm{x} \in \Omega$, для всех $s_0 \in \mathbb{R}^n$, $\mathrm{s}, \mathrm{t} \in \mathbb{R}^n$ справедливы неравенства:

$$|a_i(\mathrm{x}, s_0, \mathrm{s})| \le \widehat{a}_i(|s_0|)\left(\mathrm{P}(\mathrm{s})^{1/p_i'(\mathrm{x})} + \Phi_i(\mathrm{x})\right), \ i = 1, \ldots, n; \tag{3}$$

$$(\mathrm{a}(\mathrm{x}, s_0, \mathrm{s}) - \mathrm{a}(\mathrm{x}, s_0, \mathrm{t})) \cdot (\mathrm{s} - \mathrm{t}) > 0, \quad \mathrm{s} \ne \mathrm{t}; \tag{4}$$

$$\mathrm{a}(\mathrm{x}, s_0, \mathrm{s}) \cdot \mathrm{s} \ge \overline{a}\mathrm{P}(\mathrm{s}); \tag{5}$$

$$|b(x, s_0, \mathrm{s})| \le \widehat{b}(|s_0|)\,(\mathrm{P}(\mathrm{s}) + \Phi_0(\mathrm{x}))\,; \tag{6}$$

$$b(\mathrm{x}, s_0, \mathrm{s})\, s_0 \ge 0. \tag{7}$$

Определим пространство Соболева с переменными показателями $W^1_{\vec{\mathbf{p}}(\cdot)}(\mathbb{R}^n)$ как пополнение пространства $C_0^\infty(\mathbb{R}^n)$ по норме

$$\|v\|_{W^1_{\vec{\mathbf{p}}(\cdot)}(\mathbb{R}^n)} = \|v\|_{p_0(\cdot)} + \sum_{i=1}^{n} \|v_{x_i}\|_{p_i(\cdot)}.$$

Здесь $\|\cdot\|_{p_i(\cdot)}$ — норма Люксембурга

$$\|v\|_{L_{p_i(\cdot)}(Q)} = \|v\|_{p_i(\cdot),Q} = \inf\left\{ k > 0 \,\middle|\, \int\limits_{\mathbb{R}^n} |v/k|^{p_i(\mathrm{x})} d\mathrm{x} \le 1 \right\}$$

в пространствах Лебега с переменными показателями $L_{p_i(\cdot)}(\mathbb{R}^n)$, $i = 0, \ldots, n$.

Положим

$$T_k(r) = \begin{cases} k & \text{при } r > k, \\ r & \text{при } |r| \le k, \\ -k & \text{при } r < -k, \end{cases}$$

$\langle u \rangle = \int\limits_{\mathbb{R}^n} u d\mathrm{x}$. Через $\mathcal{T}^1_{\overrightarrow{\mathbf{p}}(\cdot)}(\mathbb{R}^n)$ обозначим множество измеримых функций $u : \mathbb{R}^n \to \mathbb{R}$ таких, что $T_k(u) \in W^1_{\overrightarrow{\mathbf{p}}(\cdot)}(\mathbb{R}^n)$ при любом $k > 0$.

Определение 1. *Энтропийным решением уравнения* (1) *называется измеримая функция* $u \in \mathcal{T}^1_{\overrightarrow{\mathbf{p}}(\cdot)}(\mathbb{R}^n)$ *такая, что* $B(\mathrm{x}) = b(\mathrm{x}, u, \nabla u) \in L_1(\mathbb{R}^n)$; *при всех* $k > 0$ *и* $\xi(\mathrm{x}) \in C_0^1(\mathbb{R}^n)$ *справедливо неравенство:*

$$\langle (b(\mathrm{x}, u, \nabla u) + |u|^{p_0(\mathrm{x})-2}u + f)\, T_k(u - \xi)\rangle + \langle \mathrm{a}(\mathrm{x}, u, \nabla u) \cdot \nabla T_k(u - \xi)\rangle \le 0.$$

Теорема. *Пусть выполнены условия* (2) – (7)*, тогда существует энтропийное решение уравнения* (1).

Определение 2. *Измеримая функция* $u \in \mathcal{T}^1_{\overrightarrow{\mathbf{p}}(\cdot)}(\mathbb{R}^n)$ *называется ренормализованным решением уравнения* (1)*, если*

$$\begin{aligned} &1) \quad B(\mathrm{x}) = b(\mathrm{x}, u, \nabla u) \in L_1(\mathbb{R}^n);\\ &2) \quad \lim\nolimits_{h\to\infty} \int\limits_{h\le|u|\le h+1} \mathrm{P}(\nabla u)\, d\mathrm{x} = 0; \end{aligned}$$

для любой функции $\xi \in W^1_{\overrightarrow{\mathbf{p}}(\cdot)}(\mathbb{R}^n) \cap L_\infty(\mathbb{R}^n)$ *и для любой гладкой функции* $S \in W^1_\infty(\mathbb{R})$ *с компактным носителем справедливо равенство:*

$$\langle (b(\mathrm{x}, u, \nabla u) + |u|^{p_0(\mathrm{x})-2}u + f(\mathrm{x}))\, S(u)\xi\rangle + \langle \mathrm{a}(\mathrm{x}, u, \nabla u) \cdot (S'(u)\xi\nabla u + S(u)\nabla\xi)\rangle = 0.$$

В работе доказано, что построенное энтропийное решение является ренормализованным решением уравнения (1). Кроме того, установлено, что если $f \le 0$ п.в. в $\mathbb{R}^n$, то $u \ge 0$ п.в. в $\mathbb{R}^n$.

Существование энтропийных решений задачи Дирихле в ограниченных областях для уравнений (1) при фиксированном росте функций $a_i(\mathrm{x}, s_0, \mathrm{s})$, $i = 1, \ldots, n$, по переменной s_0 установлено работах [2], [3]. В работе [4] введено понятие локального энтропийного решения для уравнения с p-лапласом, поглощением и мерой Радона μ:

$$\Delta_p u - |u|^{p_0-2}u = \mu, \quad p \in (1, n), \quad p < p_0.$$

В частности, M.F. Bidaut-Veron для $f \in L_{1,\mathrm{loc}}(\mathbb{R}^n)$ доказала существование локального энтропийного решения в пространстве $\mathbb{R}^n$.

Литература

1. Benilan Ph., Boccardo L., Galluet Th., Pierre M., Vazquez J. L. *An L1-theory of existence and uniqueness of solutions of nonlinear elliptic equations* // Annali della Scuola Normale Superiore di Pisa, Classe di Scienze. – 1995. – V. 22. – № 2. – P. 241–273.

2. Benboubker M. B., Hjiaj H., Ouaro S.*Entropy solutions to nonlinear elliptic anisotropic problem with variable exponent* // Journal of Applied Analysis and Computation. – 2014. – V. 4. – № 3. – P. 245–270.

3. Benboubker M. B., Chrayteh H., El Moumni M., Hjiaj H. *Entropy and renormalized solutions for nonlinear elliptic problem involving variable exponent and measure data* // Acta Mathematica Sinica, English Series. – 2015. – V. 31. – № 1. – P. 151—169.

4. Bidaut-Veron M. F. *Removable singularities and existence for a quasilinear equation with absorption or source term and measure data* // Adv. Nonlinear Stud. – 2003. – V. 3. – P. 25—63.

THE EXISTENCE OF ENTROPY SOLUTIONS OF ANISOTROPIC ELLIPTIC EQUATIONS WITH VARIABLE EXPONENTS OF NONLINEARITIES IN $\mathbb{R}^N$

A.Sh. Kamaletdinov, L.M. Kozhevnikova

In the space $\mathbb{R}^n$ we consider a certain class of anisotropic elliptic equations with variable exponents of nonlinearities and the L_1-right-hand side.The existence of entropy solutions in anisotropic Sobolev spaces with variable exponents is proved. It is established that the constructed entropy solution is a renormalized solution of the problem.

Keywords: anisotropic elliptic equation, nonlinearity variables, entropy solution, renormalized solution.

УДК 539.3, 534.1, 532.5

О КОНСЕРВАТИВНОЙ УСТОЙЧИВОСТИ УПРУГИХ И ГИДРОУПРУГИХ СИСТЕМ

Д.В. Капитанов[1], М.Е. Суслова[2], О.С. Егорова[3]

1 *dis-kdv@mail.ru*; Национальный исследовательский Нижегородский государственный университет имени Н.И. Лобачевского, Институт информационных технологий, математики и механики

2 *mariya.suslova.96@mail.ru*; Национальный исследовательский Нижегородский государственный университет имени Н.И. Лобачевского, Институт информационных технологий, математики и механики

3 *olesya.egorova.12@mail.ru*; Национальный исследовательский Нижегородский государственный университет имени Н.И. Лобачевского, Институт информационных технологий, математики и механики

Проведено исследование консервативной устойчивости шарнирно закрепленного нагруженного стерженя на упругом основании и шарнирно закрепленного трубопровода на упругом основании, транспортирующего поток жидкости с постоянной скоростью. При исследовании применяются метод разделения переменных и метод Бубнова–Галеркина с использованием функций Крылова и полиномов в качестве функций сравнения.

Ключевые слова: стержень, трубопровод, упругое основание, консервативная устойчивость.

Работа посвящена изучению консервативной устойчивости упругих и гидроупругих систем, когда потеря устойчивости не зависит от трения и других неконсервативных сил и проявляется в виде монотонного роста деформации. В отличие от неконсервативной потери устойчивости, когда исходное равновесное состояние системы сменяется движением в виде нарастающих в линейном случае колебаний, консервативная потеря устойчивости характеризуется сменой устойчивых равновесных состояний. В качестве примеров рассмотрены следующие системы: шарнирно закрепленный нагруженный стержень на упругом основании и шарнирно закрепленный трубопровод на упругом основании, транспортирующий поток жидкости с постоянной скоростью.

Исследование устойчивости шарнирно закрепленного стержня на упругом основании, как и в случае его отсутствия, проводится с помощью метода разделения переменных [1]. В результате получены выражения для вычисления критической силы и для определения номера формы, соответствующей потере устойчивости. В

случае шарнирно закрепленного трубопровода на упругом основании с помощью метода разделения переменных было получено аналитическое выражение для вычисления критического значения скорости потока жидкости для упрощенной задачи и выражение для определения номера формы, соответствующей потере устойчивости. Также для этой задачи в общем виде было проведено исследование определения критической скорости потока жидкости с использованием метода Бубнова–Галеркина. В качестве системы базисных функций берутся функции Крылова для шарнирно закрепленного стержня [2] и полиномы, удовлетворяющие граничным условиям и обладающие свойством ортонормированности. При исследовании устойчивости используется критерий Рауса–Гурвица.

Результаты исследований показали, что потеря устойчивости имеет характер дивергенции по конкретной форме деформации. Номер формы потери устойчивости зависит от коэффициента жесткости основания. Аналитическое выражение, определяющее критическую скорость потока, полученное для упрощенной модели с помощью метода разделения переменных, подтверждается исследованиями, проведенными при помощи метода Бубнова–Галеркина без этого упрощения. Результат сохраняет свое значение как при использовании трехмодового приближения, так и при использовании одномодового приближения по той форме, по которой происходит потеря устойчивости.

Работа выполнена при финансовой поддержке РНФ (грант № 16-19-10279).

Литература

1. Смирнов Л. В., Капитанов Д. В.. *Динамика упругого сжатого стержня при потере устойчивости: Учебно–методическое пособие.* – Н. Новгород: Нижегородский госуниверситет, 2010. – 20 с.

2. Коренев Б. Г., Рабинович И. М.. *Справочник по динамике сооружений.* – М.: Стройиздат, 1972. – 511 с.

CONSERVATIVE LOSS OF STABILITY IN ELASTIC AND HYDRO ELASTIC SYSTEMS

D.V. Kapitanov, M.E. Suslova, O.S. Egorova

We study conservative stability of a loaded articulated rod on an elastic base and an articulated pipeline on an elastic base which transports liquid with a constant speed. The method of separation of variables and the Bubnov-Galerkin method with the Krylov functions and polynomials as a comparison functions has been used.

Keywords: rod, pipeline, elastic base, conservative stability.

УДК 517.53/.55

О ДОСТАТОЧНЫХ УСЛОВИЯХ ПОЛНОТЫ ЭКСПОНЕНЦИАЛЬНОЙ СИСТЕМЫ В ВЫПУКЛЫХ ОБЛАСТЯХ

А.Ф. Кужаев[1]

1 *arsenkuzh@outlook.com*; Башкирский государственный университет

Приводятся достаточные условия полноты системы экспоненциальных мономов в выпуклых областях. Данный результат является обобщением классического утверждения, полученного независимо друг от друга А.Ф. Леонтьевым и Б.Я. Левиным, на случай показателей, не имеющих плотность. Выяснено, что ослаблением условия измеримости последовательности (то есть существования плотности) в контексте упомянутого выше результата о полноте, является равенство верхней и максимальной плотностей.

Ключевые слова: плотность последовательности, целая функция, полнота, выпуклая область.

Пусть $\Lambda = \{\lambda_k, n_k\}_{k=1}^{\infty}$ — кратная последовательность положительных чисел. Здесь $\{\lambda_k\}_{k=1}^{\infty}$ — неограниченная строго возрастающая последовательность положительных чисел, и n_k — натуральное число, называемое кратностью элемента $\lambda_k, k \in \mathbb{N}$. Напомним, что *верхней плотностью* и *максимальной плотностью* соответственно называется следующие характеристики последовательности Λ:

$$\bar{n}(\Lambda) := \varlimsup_{t\to+\infty} \frac{1}{t} \sum_{\lambda_k \leqslant t} n_k, \quad \bar{n}_0(\Lambda) := \lim_{\delta\to 0+} \varlimsup_{t\to+\infty} \frac{1}{\delta t} \sum_{t(1-\delta)<\lambda_k\leqslant t} n_k.$$

Согласно [1, §E3, гл. IV] предел по $\delta \to 0+$ всегда существует, так что максимальная плотность определена корректно.

В случае существования предела

$$n(\Lambda) := \lim_{t\to+\infty} \frac{1}{t} \sum_{\lambda_k \leqslant t} n_k$$

последовательность Λ называют *измеримой*, а данный предел — просто *плотностью*.

Если последовательность Λ измерима, то верхняя и максимальная плотности для неё сопадают и равны плотности [2, лемма 2.1]. Нас будет интересовать случай, когда у последовательности Λ совпадают верхняя и максимальная плотности, но при этом последовательность не является измеримой. Множество таких последовательностей непусто, что демонстрирует следующий пример.

Пусть $0 < R_k \to \infty, k \to \infty$, и $R_{k+1}/R_k \to \infty, k \to \infty$. Положим $\Lambda = \bigcup_{k\in\mathbb{N}} \Lambda_k$, где Λ_k — множество, состоящее из всех натуральных чисел, принадлежащих интервалу $(R_{2k}; R_{2k+1}), k \in \mathbb{N}$, кратность каждого из которых равна единице. Положим для краткости

$$n(t, \Lambda) = \sum_{\lambda_k \leqslant t} n_k.$$

В силу выбора чисел R_k имеем:

$$\bar{n}(\Lambda) = \overline{\lim_{t\to+\infty}} \frac{n(t,\Lambda)}{t} \geqslant \lim_{k\to\infty} \frac{n(R_{2k+1},\Lambda)}{R_{2k+1}} \geqslant \lim_{k\to\infty} \frac{R_{2k+1}-R_{2k}}{R_{2k+1}} = 1.$$

Пусть $\delta \in (0;1)$. Обозначим

$$\bar{n}_0(\Lambda,\delta) = \overline{\lim_{t\to+\infty}} \frac{n(t,\Lambda)-n(t(1-\delta),\Lambda)}{\delta t}.$$

Тогда

$$\bar{n}_0(\Lambda,\delta) = \lim_{k\to\infty} \frac{n(R_{2k+1},\Lambda)-n(R_{2k+1}(1-\delta),\Lambda)}{\delta R_{2k+1}} = \lim_{k\to\infty} \frac{\delta R_{2k+1}}{\delta R_{2k+1}} = 1.$$

Отсюда с учетом предыдущего согласно [3, лемма 1] получаем: $\bar{n}_0(\Lambda) = \bar{n}(\Lambda)$. В то же время имеем:

$$\underline{\lim_{t\to+\infty}} \frac{n(t,\Lambda)}{t} = \lim_{k\to\infty} \frac{n(R_{2k},\Lambda)}{R_{2k}} \leqslant \lim_{k\to\infty} \frac{R_{2k-1}}{R_{2k}} = 0.$$

Таким образом, последовательность Λ не имеет плотности.

Пусть G — произвольная выпуклая область комплексной плоскости. *Вертикальным диаметром области G* будем называть следующую величину:

$$d(G) := \sup_x \sup_{z_1,z_2\in G} \left\{ |y_1-y_2| : z_1 = x+iy_1, z_2 = x+iy_2, \quad z_1,z_2\in G, \quad x\in\mathbb{R} \right\}.$$

Через $K_G(\varphi)$ будем обозначать опорную функцию выпуклой области G ([4, стр. 43])

Положим $\mathscr{E}(\Lambda) = \{z^l e^{\lambda_k z}\}_{k=1,l=0}^{\infty,n_k-1}$. Будем говорить, что *система функций $\mathscr{E}(\Lambda)$ полна в выпуклой области G*, если она полна в пространстве функций, аналитических в области G с топологией равномерной сходимости на компактных подмножествах из G.

Следующее утверждение даёт обобщение классического результата Левина-Леонтьева, который был получен ими независимо друг от друга ([5, стр. 286], [4, стр. 122]).

Теорема. *Пусть $\bar{n}(\Lambda) = \bar{n}_0(\Lambda) = \tau < \infty$. Тогда система $\mathscr{E}(\Lambda)$ полна в любой области G, для которой выполнено условие*

$$K_G\left(-\frac{\pi}{2}\right) + K_G\left(\frac{\pi}{2}\right) = d(G) \leqslant 2\pi\tau,$$

и неполна в любой области G с вертикальным диаметром $d(G) > 2\pi\tau$.

Литература

1. Koosis P. *The logarithmic integral I.* – Cambridge University Press, 1997. – 625 p.

2. Абдулнагимов А. И., Кривошеев А. С. *Правильно распределенные подмножества в комплексной плоскости* // Алгебра и анализ. – 2016. – Т. 28. – № 4. – С. 1–46.

3. Кривошеев А. С., Кужаев А. Ф *Об одной теореме Леонтьева-Левина* // Уфимский матем. ж. – 2017. – Т. 9. – № 3. – С. 89–101.

4. Леонтьев А. Ф. *Целые функции. Ряды экспонент.* – М.: Наука, 1983. – 176 с.

5. Левин Б. Я. *Распределение корней целых функций.* – М.: ГИТТЛ, 1956. –632 с.

ON SUFFICIENT CONDITIONS OF THE COMPLETENESS OF EXPONENTIAL SYSTEMS IN CONVEX DOMAINS

A.F. Kuzhaev

We give some sufficient conditions for the completeness of the system of exponential monomials in convex domains. This result is a generalization of a classical proposition on completeness of exponential monomials systems with positive exponents in a convex domain when these exponents have not density. The proposition was obtained by A. Leontiev and B. Levin independently. It is discovered that the condition of sequence's measurability (i.e. existence of its density) can be replaced by the condition of equality of its upper and maximum densities.

Keywords: density of sequence, entire function, completeness, convex domain.

УДК 519.62

СТРУКТУРА ГЛОБАЛЬНОГО АТТРАКТОРА ОБОБЩЕННОЙ СИСТЕМЫ ЧУА

О.И. Кузнецова[1]

1 *oxxy4893@mail.ru*; Тульский государственный университет, Институт прикладной математики и компьютерных наук

В статье рассматривается проблема поиска неустойчивых траекторий в автономных системах дифференциальных уравнений. Приводятся результаты работы метода стрельбы для обобщенной системы Чуа, благодаря которому можно отыскать неустойчивые траектории в динамической системе.

Ключевые слова: трехмерные динамические системы, неустойчивые траектории, численные методы, метод стрельбы, итерационные методы.

Известен ряд катастроф летательных аппаратов, вызванных неправильным синтезом алгоритмов управления: катастрофы американского многоцелевого истребителя YF-22 «Раптор», который потерпел крушение при посадке на авиабазе Эдвардс в апреле 1992 года, и шведского истребителя «Грифон». Эти катастрофы были вызваны неправильным синтезом алгоритмов управления, которое производилось без учета нелинейностей типа «насыщение», влияние которых может вызвать т.н. «колебания, вызванные летчиком», нарушающие процесс пилотирования ЛА. В них наблюдался эффект «флаттера по тангажу» в режиме приземления самолетов (т.е. возникали колебания угла тангажа с нарастающей амплитудой).

Хорошо также известны случаи входа космического аппарата в неконтролируемое вращение. Исследования переходных режимов при гашении подобного вращения приводит к необходимости разработки математической теории глобального анализа систем ориентации. На необходимость развития такой теории указывал академик Б.В. Раушенбах, отмечая сложности управления космическим аппаратом при быстрых разворотах.

При исследовании математических моделей систем управления полетом самолета и ракеты при учете "насыщения" обнаруживаются так называемые скрытые аттракторы, наличие которых и приводит к катастрофическим последствиям [2].

Рассмотрим обобщенную систему Чуа [1]

$$\begin{cases} \dot{x} = \alpha(y - x) - \alpha\phi(x), \\ \dot{y} = x - y + z, \\ \dot{z} = -\beta y + \gamma z, \end{cases} \tag{1}$$

с нелинейностью вида

$$\phi(x) = m_1 x + 0.5(m_0 - m_1)(|x+1| - |x-1|) + 0.5(s - m_0)(|x+\delta_0| - |x-\delta_0|) \tag{2}$$

и следующими значениями параметров:

$$\alpha = 8.4562, \beta = 12.0732, \gamma = 0.0052, m_0 = 0.14, m_1 = -1.1468, s = -0.9668, \delta_0 = 0.2. \tag{3}$$

Система (1) с нелинейностью (2) и параметрами (3) устойчива в малом. С использованием алгоритма, предложенного в [1], для поиска скрытого аттрактора обобщенной системы Чуа, а также соображений из [3], был найден глобальный аттрактор (рис. 1), который состоит из трех устойчивых циклов и двух неустойчивых.

Рис. 1.

Литература

1. Burkin I.M., Khien N. *Analytical-numerical methods of finding hidden oscillations in multidimensional dynamical systems* // Differential Equations. – 2014. – V. 50, no. 13. – P. 1695–1717.

2. Leonov G. A., Kuznetsov N.V., Vagaitsev V.I. *Localization of hidden chuas attractors* // Phys Lett. App. – 2011. – No. 375. – P. 2230–2233.

3. Кузнецова О.И. *Локализация неустойчивых траекторий многомерных динамических систем дифференциальных уравнений методом простой стрельбы* // Вест. Тульск. гос. ун-та. – 2015. – № 1. – С. 26–34.

STRUCTURE OF THE GLOBAL ATTRACTOR OF THE GENERALIZED CHUA SYSTEM

O.I. Kuznetsova

We consider the problem of finding unstable orbits in autonomous systems of differential equations. The results of reberty shooting method for the generalized Chua system are given, through which it is

possible to find an unstable trajectory in a dynamic system.
Keywords: three-dimensional dynamical systems, unstable trajectories, numerical methods, shooting method, iterative methods.

УДК 517.5

ОБ ОДНОМ АНАЛОГЕ ИНТЕГРАЛЬНОЙ ФОРМУЛЫ ПЛАНА

В.И. Кузоватов[1]

1 *kuzovatov@yandex.ru*; Сибирский федеральный университет

В работе получен аналог формулы Плана, которая имеет существенное значение при нахождении функционального соотношения для классической дзета-функции Римана.

Ключевые слова: формула Плана, целая функция, интегральное представление.

Целью данной работы является получение аналога формулы Плана, которая имеет существенное значение при нахождении функционального соотношения для классической дзета-функции Римана.

Классическая формула Плана выражает сумму значений в целых точках голоморфной и ограниченной (для всех значений z, для которых $x_1 \le \mathrm{Re}\, z \le x_2$, x_1, x_2 – целые числа) функции $\varphi(z)$ через некоторые интегралы. А именно,

$$\frac{1}{2}\varphi(x_1) + \varphi(x_1+1) + \varphi(x_1+2) + \ldots + \varphi(x_2-1) + \frac{1}{2}\varphi(x_2) =$$
$$= \int_{x_1}^{x_2} \varphi(z)\, dz + \frac{1}{i}\int_0^{\infty} \frac{\varphi(x_2+iy) - \varphi(x_2-iy) + \varphi(x_1-iy) - \varphi(x_1+iy)}{e^{2\pi y}-1}\, dy.$$

Если говорить об обобщениях дзета-функции, то И.М. Гельфанд, Б.М. Левитан и Л.А. Дикий изучали дзета-функцию, ассоциированную с собственными значениями оператора Штурма-Лиувилля в 50-х годах прошлого века. Ее значение оказалось связанным со следом данного оператора. Их подход был развит далее В.Б. Лидским и В.А. Садовничим (60 годы), которые рассмотрели класс целых функций одного переменного, определили для них дзета-функцию корней и исследовали ее область аналитического продолжения. С.А. Смагин и М.А. Шубин построили дзета-функцию эллиптических операторов и операторов более общего вида, доказали возможность мероморфного продолжения дзета-функции и дали некоторую информацию о полюсах.

Пусть $f(z)$ – целая функция порядка ρ в $\mathbb{C}$. Рассмотрим уравнение

$$f(z) = 0. \tag{1}$$

Обозначим через $N_f = f^{-1}(0)$ множество всех корней уравнения (1) (каждый корень считается столько раз, какова его кратность). Число корней не более чем счетно.

Дзета-функция $\zeta_f(s)$ корней уравнения (1) определяется следующим образом:

$$\zeta_f(s) = \sum_{a \in N_f} (-a)^{-s},$$

где $s \in \mathbb{C}$. Знак минус в определении дзета-функции взят для удобства записи интегральных формул.

Приведем интегральное представление для дзета-функции $\zeta_f(s)$ нулей z_n функции f, которые имеют вид

$$z_n = -q_n + is_n, \quad q_n > 0.$$

Обозначим

$$F(f,x) = \sum_{n=1}^{\infty} e^{z_n x} \tag{2}$$

и предположим, что $\operatorname{Re} s = \sigma > 1$ и выполнены следующие условия:

$$\varliminf_{n\to\infty} \frac{q_n}{n} > 0, \tag{3}$$

$$\text{ряд} \quad \sum_{n=1}^{\infty} \left(\frac{1}{q_n}\right)^{\sigma-1} \text{сходится.} \tag{4}$$

Для сходимости ряда (2), с учетом (3), необходимо и достаточно, чтобы $x > 0$.

Теорема. *Пусть выполнены условия (3), (4) и* $\operatorname{Re} s > 1$. *Тогда*

$$\zeta_f(s) = \frac{1}{\Gamma(s)} \int_0^{\infty} x^{s-1} F(f,x)\, dx,$$

где $F(f,x)$ *определяется формулой (2).*

В данной работе будем предполагать, что нули z_n имеют вид

$$z_n = -q_n, \quad q_n > 0,$$

где q_n образуют некоторую последовательность натуральных чисел.

Рассмотрим функцию

$$F(f, 2\pi i z) = \sum_{n=1}^{\infty} e^{z_n 2\pi i z} = \sum_{n=1}^{\infty} e^{-q_n 2\pi i z}. \tag{5}$$

Областью сходимости ряда $F(f, 2\pi i z)$, определенного формулой (5), является множество, задаваемое условием $y < 0$.

При помощи замены $e^{-2\pi i z} = w$ ряд (5) приводится к виду $\sum\limits_{n=1}^{\infty} w^{q_n}$ или

$$G(w) = \sum_{n=1}^{\infty} f_n w^n, \tag{6}$$

где коэффициенты f_n определяются следующим образом:

$$f_n = \begin{cases} 1, & n = q_k \\ 0, & n \neq q_k, \end{cases} \quad \text{поэтому} \quad \varlimsup_{n\to\infty} \sqrt[n]{|f_n|} = 1.$$

Заметим, что в ряде (6) бесконечное число коэффициентов f_n отлично от нуля.

При $|w| \to 1-0$ функция $G(w)$ становится неограниченной, но является голоморфной в единичном круге. Таким образом, $G(w)$ не продолжается в точку 1. Теорема Фабри о лакунах показывает, что можно подобрать коэффициенты ряда так, что у полученной функции $G(w)$ вся окружность будет являться естественной границей.

В дальнейшем ограничимся рассмотрением классов рациональных функций $G(w)$, для которых справедливо представление (6). Относительно этого сформулируем следующий результат.

Теорема Сеге. *Степенной ряд*

$$G(w) = \sum_{0}^{\infty} f_n w^n, \tag{7}$$

коэффициенты которого f_n могут принимать лишь конечное число различных значений, или представляет собой рациональную функцию, или непродолжаем за пределы единичного круга. В случае рациональности суммы ряда (7)

$$G(w) = \frac{P(w)}{1-w^N},$$

где $P(w)$ — многочлен, а N — некоторое натуральное число.

Это означает, что особыми точками (в данном случае полюсами первого порядка) для функции $G(w)$ могут быть только точки

$$w_k = e^{i\frac{2\pi}{N}k}, \quad k = 0, 1, \ldots, N-1, \quad N \in \mathbb{N}.$$

В переменных z для функции $F\left(f, 2\pi i z\right)$ особыми точками будут точки

$$e^{-2\pi i z} = w_k, \quad -2\pi i z = i\left(\frac{2\pi}{N}k + 2\pi l\right), \quad z = -\left(\frac{k}{N} + l\right), \quad l = 0, \pm 1, \pm 2, \ldots,$$

или что то же самое

$$z_{k,l} = l - \frac{k}{N}, \quad l = 0, \pm 1, \pm 2, \ldots, \quad k = 0, 1, \ldots, N-1.$$

Пусть для q_n выполнено соотношение (3). Предположим дополнительно, что $\deg P(w) = N$, то есть

$$P(w) = a_1 w + a_2 w^2 + \ldots + a_{N-1} w^{N-1} + w^N,$$

где коэффициенты $a_j \in \{0, 1\}$ ввиду разложения (6), $j = 1, \ldots, N-1$.

Если $\deg P(w) > N$, то в выражении для $G(w)$ можно выделить целую часть, которая будет содержать лишь конечное число слагаемых, и на элементы $G(w)$, начиная с некоторого номера, эти слагаемые оказывать влияния не будут. Если $\deg P(w) \leq N$, то в разложении $G(w)$ будут коэффициенты многочлена $P(w)$, которые будут периодически повторяться (ввиду геометрической прогрессии). Моном w^N выделен для удобства вычислений.

Приведем явное выражение функции $F\left(f,2\pi iz\right)$ через функцию $G(w)$. Будем иметь

$$F\left(f,2\pi iz\right)=\frac{P\left(e^{-2\pi iz}\right)}{1-e^{-2\pi izN}}. \tag{8}$$

Отметим, что выражение (8) является аналитическим продолжением введенной ранее функции $F\left(f,2\pi iz\right)$, определяемой по формуле (5). Областью определения выражения (8) является комплексная плоскость $\mathbb{C}$ за исключением особых точек $z_{k,l}$.

Основным результатом работы является следующее утверждение.

Теорема. *Пусть x_1 и x_2 — целые числа, а $\varphi(z)$ — функция, голоморфная и ограниченная на множестве $\{x_1 \le \mathrm{Re}\ z \le x_2\}$. Тогда*

$$\begin{aligned}
&\frac{P(w_0)}{N}\left(\frac{1}{2}\varphi(x_1)+\varphi(x_1+1)+\varphi(x_1+2)+\ldots+\varphi(x_2-1)+\frac{1}{2}\varphi(x_2)\right)+\\
&+\frac{P(w_1)}{N}\left(\varphi\big(x_1+1-\frac{1}{N}\big)+\varphi\big(x_1+2-\frac{1}{N}\big)+\ldots+\varphi\big(x_2-1-\frac{1}{N}\big)+\varphi\big(x_2-\frac{1}{N}\big)\right)+\\
&+\frac{P(w_2)}{N}\left(\varphi\big(x_1+1-\frac{2}{N}\big)+\varphi\big(x_1+2-\frac{2}{N}\big)+\ldots+\varphi\big(x_2-1-\frac{2}{N}\big)+\varphi\big(x_2-\frac{2}{N}\big)\right)+\\
&+\ldots+\\
&+\frac{P(w_{N-1})}{N}\left(\varphi\big(x_1+1-\frac{N-1}{N}\big)+\varphi\big(x_1+2-\frac{N-1}{N}\big)+\ldots+\varphi\big(x_2-1-\frac{N-1}{N}\big)+\right.\\
&\left.+\varphi\big(x_2-\frac{N-1}{N}\big)\right)=\\
&=\int_{x_1}^{x_2}\varphi(z)\,dz+\frac{1}{i}\int_0^{\infty}\Big(\varphi\left(x_1-iy\right)F\left(f,2\pi y\right)+\varphi\left(x_1+iy\right)\left[1+F\left(f,-2\pi y\right)\right]\Big)dy-\\
&-\frac{1}{i}\int_0^{\infty}\Big(\varphi\left(x_2-iy\right)F\left(f,2\pi y\right)+\varphi\left(x_2+iy\right)\left[1+F\left(f,-2\pi y\right)\right]\Big)dy.
\end{aligned}$$

Здесь $F\left(f,2\pi y\right)=\sum\limits_{n=1}^{\infty}e^{-q_n 2\pi y}$.

Работа выполнена при финансовой поддержке РФФИ (проекты 15-01-00277, 16-31-00173).

ON ONE ANALOG OF THE INTEGRAL PLAN FORMULA

V.I. Kuzovatov

In this paper we present an analog of the Plan formula, which is essential in obtaining a functional relation to the classical Riemann zeta-function.

Keywords: plan formula, entire function, integral representation.

УДК 519.6

ИССЛЕДОВАНИЕ ПОВЕДЕНИЯ КУСОЧНО-ЛИНЕЙНОГО ОТОБРАЖЕНИЯ НА ГРАНИЦАХ СМЕЖНЫХ ОБЛАСТЕЙ С РАЗНОЙ ДИНАМИКОЙ

А.В. Малышко[1], Т.А. Трифонова[2]

1 *anna.trifonowa2012@yandex.ru*; Казанский национальный исследовательский технический университет им. А.Н. Туполева

2 *anna.trifonowa2012@yandex.ru*; Казанский национальный исследовательский технический университет им. А.Н. Туполева

В работе изучается динамическая система, заданная одномерным кусочно-линейным отображением с двумя параметрами. Проведено исследование поведения данного отображения на границах смежных областей значений параметров, где система имеет разную динамику.

Ключевые слова: динамическая система, кусочно-линейное отображение с двумя параметрами, граничный переход.

В настоящее время все активнее изучаются дискретные динамические системы, порожденные кусочно-линейными и кусочно-гладкими одномерными отображениями. Математические модели, построенные с помощью таких систем, находят широкое применение в радиофизике, робототехнике, энергетике, экономике, экологии, исследовании закономерностей развития финансовых рынков, описании биологических популяций.

Для задач прикладного характера большой интерес представляют исследования дискретных динамических систем, определяемых кусочно-линейными отображениями, заданными с помощью трех или более линейных функций. Особое внимание уделяется изучению динамики отображений с параметрами, в том числе, их хаотического поведения, а также изменения поведения системы при переходах через границы смежных областей с разной динамикой [1–4].

В работе исследованы особенности поведения динамической системы, порожденной кусочно-линейным отображением f, на границах смежных областей параметров, где отображение имеет различную динамику. Это отображение является достаточно общим кусочно-линейным отображением, задаваемым тремя различными линейными функциями с двумя параметрами p и q.

В ходе исследования неподвижных и двупериодических точек плоскость значений параметров (p, q) была разбита на области с одинаковой динамикой. Для границ смежных областей проведено исследование динамического поведения отображения f, определены условия существования притягивающих и отталкивающих неподвижных точек и периодических орбит. Построены паутинные и бифуркационные диаграммы, соответствующие границам областей с различной динамикой отображения. Наиболее интересные результаты получены на границах областей значений параметров, при которых поведение отображения f носит хаотический характер.

Литература

1. Sushko I. et al. *Bifurcation structure of parameter plane for a family of unimodal piecewise smooth maps: Border-collision bifurcation curves* // In: Bischi, G.I. & Sushko I. (eds.) Dynamic Modelling in Economics and Finance. Chaos Solit. Fract., 2006.

2. Jianxin Liu, Xuan Zhang, Zhiming Li, Xuling Li. *A tent map based conversion circuit for robot tactile sensor* // Journal of Sensors. – 2013. – V. 2013. – 5 p.

3. Wang Shuang-xin, Li Han, Zhang Xiu-xia, Wang Zhi-qin. *Nonlinear predictive load control of boiler-turbine-generating unit based on chaos optimization* // 2nd Chaotic Modeling and Simulation Int. Conf. – Crete, Greece, 1–5 June, 2009.

4. Tramontana F., Gardini L., Westerhoff F. *Intricate asset price dynamics and one-dimensional discontinuous maps* // In: Puu T., Panchuck A. (eds.) Advances in nonlinear economic dynamics. Nova Science Publishers, 2010.

BEHAVIOUR INVESTIGATION OF PIECEWISE LINEAR MAP ON THE BORDERS OF COMPLEMENTARY AREAS WITH DIFFERENT DYNAMICS

A.V. Malyshko, T.A. Trifonova

In the paper, a dynamic system given by a piecewise linear map with two parameters is considered. It is investigated behavior of the map on the boundary of two adjacent domains having distinct dynamics.

Keywords: dynamical system, piece-wise linear map with two parameters, border collisions.

УДК 519.7; 512.581

ОБ АНАЛОГАХ ПРОТОКОЛА MOR ФОРМИРОВНИЯ ОБЩЕГО СЕКРЕТНОГО КЛЮЧА, ОСНОВАННЫХ НА 2-КАТЕГОРИЯХ

С.Н. Мальцева[1]

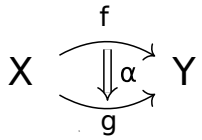
1 *fofka1994@yandex.ru*; Казанский (Приволжский) федеральный университет, Институт математики и механики

Строится протокол формирования общего секретного ключа на платформе 2-категорий.

Ключевые слова: криптография, 2-категории, протокол формирования общего секретного ключа, MOR.

В данной работе модифицируется известный протокол MOR [1, с. 57], [2]. Основой модификации является использование новой алгебраической платформы — 2-категорий. Определение 2-категорий можно найти, например, в книге [3, с. 312]. Мы рассмотрим четыре варианта протокола формирования общего секретного ключа, которые похожи на протокол MOR. Вертикальное умножение 2-морфизмов в 2-категории будет обозначаться точкой, горизонтальное — кружочком.

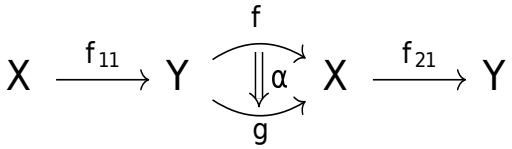
Рассмотрим первый вариант протокола формирования общего секретного ключа. Пусть имеются открытые данные: 2-категория $\mathfrak{K}$, 2-стрелка вида



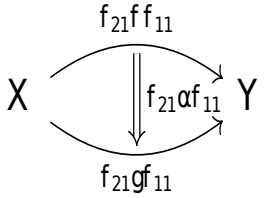
Будем предполагать, что в полугруппах с единицей $G_1 = \mathfrak{K}(X, X)$, $G_2 = \mathfrak{K}(Y, Y)$ (это 1-стрелки) имеются пары больших полугрупп $G_{11}, G_{12} \subset G_1, G_{21}, G_{22} \subset G_2$, элементы которых коммутируют между собой, т.е. если $f_{ij} \in G_{ij}$, то $f_{11}f_{12} = f_{12}f_{11}, f_{21}f_{22} = f_{22}f_{11}$.

Протокол

1. Алиса случайным образом выбирает $f_{11} \in G_{11}, f_{21} \in G_{21}$, вычисляет 2-морфизм

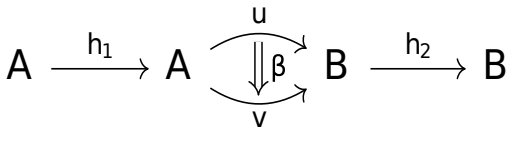


и посылает Бобу $\alpha_1 = f_{21}\alpha f_{11}$:

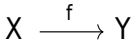


2. Также Боб случайным образом выбирает $f_{12} \in G_{12}, f_{22} \in G_{22}$, вычисляет 2-морфизм $\alpha_2 = f_{22}\alpha f_{12}$, и посылает Алисе.
3. Алиса вычисляет $\lambda_1 = f_{21}\alpha_2 f_{11}$
4. Боб вычисляет $\lambda_2 = f_{22}\alpha_1 f_{12}$.
Из условий на G_{ij} следует, что $\lambda_1 = \lambda_2$ — общий секретный ключ.

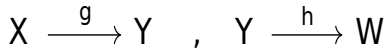
Криптостойкость основана на сложности нахождения h_1 и h_2 из известных β и $h_2\beta_1$, где



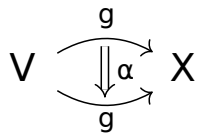
Ко всему прочему мы можем воспользоваться вертикальной композицией. Это будет второй вариант протокола, похожего на MOR. Открыт 1-морфизм



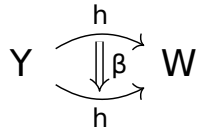
и 1-морфизмы



Имеются две полугруппы с единицами:
G_1 — 2-морфизмы вида



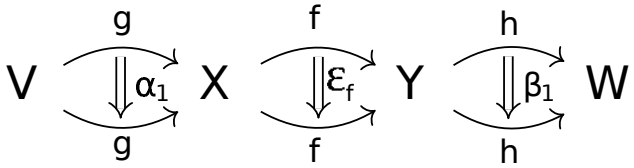
G_2 — 2-морфизм вида



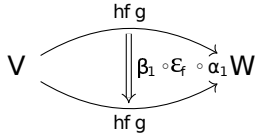
В этих полугруппах предполагается существование полугрупп $G_{11}, G_{12} \subset G_1, G_{21}, G_{22} \subset G_2$, морфизмы из которых коммутируют: если $\alpha_1 \in G_{11}, \alpha_2 \in G12$, то $\alpha_1\alpha_2 = \alpha_2\alpha_1, \beta_1 \in G_{21}, \beta_2 \in G_{22}$, то $\beta_1\beta_2 = \beta_2\beta_1$. Эти полугруппы должны быть большими, чтобы исключить возможность атаки “грубой силой” (т.е. перебором всех вариантов).

Протокол

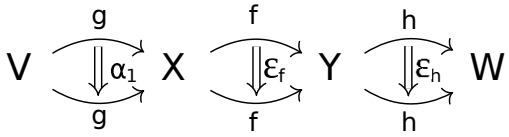
1. Алиса случайным образом выбирает $\alpha \in G_{11}, \beta \in G_{21}$
и вычисляет $\gamma_1 = \beta_1 \circ \epsilon_f \circ \alpha_1$



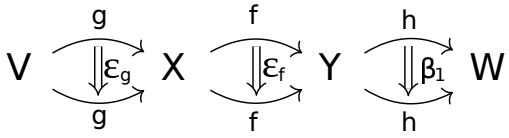
2-морфизм γ_1 посылается Бобу:



2. Аналогично Боб выбирает $\alpha_2 \in G_{12}, \beta_2 \in G_{22}$, вычисляет $\gamma_2 = \beta_2 \circ \epsilon_g \circ \alpha_2$, и посылает Алисе.
3. Алиса вычисляет вертикальную композицию γ_2 с морфизмами $\epsilon_h \circ \epsilon_f \circ \alpha_1 = \epsilon_{hf} \circ \alpha_1$



и



$\beta_1 \circ \epsilon_f \circ \epsilon_y = \beta_1 \circ \epsilon_{fg}$

То есть $\lambda_1 = (\beta_1 \circ \epsilon_f \circ \epsilon_g) \cdot \gamma_2 \cdot (\epsilon_h \circ \epsilon_f \circ \alpha_1) = (\beta_1 \circ \epsilon_f \circ \epsilon_g) \cdot (\beta_2 \circ \epsilon_f \circ \alpha_2) \cdot (\epsilon_h \circ \epsilon_f \circ \alpha_1)$

Используя свойство, которое связывает вертикальную и горизонтальную композицию $(\mu \circ \nu) \cdot (\sigma \circ \tau) = (\mu \cdot \sigma) \circ (\nu \cdot \tau)$, вычислим $(\beta_1 \circ \epsilon_{fg}) \cdot (\beta_2 \circ (\epsilon_f \circ \alpha_2)) = (\beta_1 \cdot \beta_2) \circ (\epsilon_{fg} \cdot (\epsilon_f \circ \alpha_2)) = (\beta_1 \cdot \beta_2) \circ (\epsilon_f \circ \alpha_2)$, так как ϵ_{fg} – вертикальная единица.

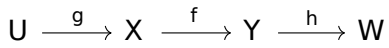
Вычисляем $\lambda_1 = ((\beta_1 \cdot \beta_2) \circ (\epsilon_f \circ \alpha_2)) \cdot (\epsilon_h \circ (\epsilon_f \circ \alpha_1)) = ((\beta_1 \cdot \beta_2) \circ (\epsilon_f \circ \alpha_2)) \cdot (\epsilon_{hf} \circ \alpha_1) = ((\beta_1 \cdot \beta_2) \cdot \epsilon_h) \circ ((\epsilon_f \circ \alpha_2) \cdot (\epsilon_f \circ \alpha_1)) = (\beta_1 \cdot \beta_2) \circ ((\epsilon_f \cdot \epsilon_f) \circ (\alpha_2 \cdot \alpha_1)) = (\beta_1 \cdot \beta_2) \circ \epsilon_f \circ (\alpha_2 \cdot \alpha_1)$

Аналогично, пусть $\lambda_2 = (\beta_2 \circ \epsilon_f \circ \epsilon_g) \cdot \gamma_1 \cdot (\epsilon_h \circ \epsilon_f \circ \alpha_2)$

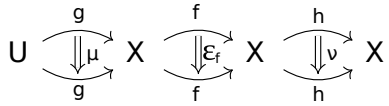
Если произвести подобные вычисления, что и с λ_1, получим $\lambda_2 = (\beta_2 \cdot \beta_1 \circ \epsilon_f \circ (\alpha_1 \cdot \alpha_2))$

Но так как $\beta_1 \cdot \beta_2 = \beta_2 \cdot \beta_1$, и $\alpha_1 \cdot \alpha_2 = \alpha_2 \cdot \alpha_1$, то $\lambda_1 = \lambda_2$ — это общий секретный ключ.

Криптостойкость основана на сложности задачи о нахождении μ и nu, если известны f, g, h



и горизонтальная композиция:



т.е. $\nu \circ \epsilon_f \circ \mu$.

Третий вариант протокола будет похож на первый вариант, но предполагается, что $X = Y, G_{11} = G_{21}$ и $G_{12} = G_{22}$ – группы. При этом $f_{21} = f_{11}^{-1}, f_{22} = f_{12}^{-1}$.

Рассмотрим последний вариант протокола, похожего на MOR. Этот вариант похож на второй вариант, но предполагается, что $V = X = Y = W, G_{11} = G_{21}, G_{12} = G_{22}$ – группы, а $\beta_1 = \alpha_1^{-1}$ (относительно вертикальной композии)$\beta_2 = \alpha_2^{-1}$

Литература

1. Романьков В. А. *Алгебраическая криптография.* – Омск: Изд-во Омск. гос. ун-та, 2013. – 136 с.

2. Mahalanobis A. *A simple generalization of the El-Gamal cryptosystem to non-abelian groups* // arXiv:cs/0607011v5 [cs.CR] 7 May 2007. — 13 p.

3. Маклейн С. *Категории для работающего математика.* – Москва: ФИЗМАТЛИТ, 2004. – 352 с.

ON ANALOGUES OF THE KEY EXCHANGE MOR PROTOCOL BASED ON 2-CATEGORIES

S.N. Maltseva

In this paper, a key exchange protocol of MOR type is created on the platform of 2-categories.

Keywords: key exchange protocol, 2-category, MOR.

УДК 519.6

ПРИМЕНЕНИЕ ДИСКРЕТНЫХ ДИНАМИЧЕСКИХ СИСТЕМ К ИЗУЧЕНИЮ ПОПУЛЯЦИОННЫХ МОДЕЛЕЙ

Е.Н. Матвеева[1], Н.И. Насырова[2]

1 *ngoza@yandex.ru*; Северный (Арктический) федеральный университет
2 *ngoza@yandex.ru*; Казанский национальный исследовательский технический университет им. А.Н. Туполева

В работе проведено исследование динамики отображения $f(x) = rxe^{-x}$, $x \in \mathbb{R}$, в зависимости от значения параметра $r \in \mathbb{R} \setminus \{0\}$. Интерпретированы результаты аналитического исследования данного отображения для биологической модели Рикера и выявлены значения параметра r, при которых наблюдается наиболее благоприятная ситуация для развития рыбной популяции, прогноза ее численности и промыслового улова.

Ключевые слова: дискретная динамическая система, биологическая популяция, модель Рикера.

Дискретные динамические системы, порожденные гладкими и кусочно-гладкими одномерными отображениями с одним или двумя параметрами все чаще применяют при построении математических моделей в задачах прикладного характера. Например, изменение численности биологической популяции может быть описано с помощью логистической модели или модели Бивертона-Холта, симметрического или асимметрического тентообразного отображения, моделей двумерной дискретной динамики.

Еще одной интересной моделью, описывающей популяции, является модель Рикера (Ricker), которая показывает зависимость пополнения (рекрутов) рыбной популяции от родительского запаса. График зависимости числа рекрутов от численности производителей называется кривой пополнения. Семейство кривых, предложенных в 1954 г. ихтиологом У.Е. Рикером, можно описать различными выражениями, основное из которых имеет вид $R = \alpha P e^{-\beta P}$, где R – число рекрутов (численность пополнения популяции); P – величина родительского запаса (измеренная в

штуках, единицах массы, в количестве отложенной икры, и т. д.); α – скорость роста популяции в отсутствии лимитирования (безразмерный параметр); β – параметр с размерностью $1/P$ (связан с емкостью экологической ниши данной популяции).

Кривая пополнения Рикера применима при изучении рыбных популяций, когда в результате высокой плотности рыбе требуется больше времени, чтобы вырасти до промысловых размеров; когда реакция хищников и паразитов на численность молодых потребляемых ими рыб запаздывает по времени, так что у вида-жертвы с высокой первоначальной плотностью возникает перекомпенсация численности.

При исследовании модели Рикера $R = \alpha P e^{-\beta P}$ можно видеть, что параметр β в уравнении не влияет на характер динамического поведения. Действительно, если ввести преобразование переменной $x = \beta P$, то получим уравнение $f(x) = rxe^{-x}$, $\alpha = r$.

Нами проведено исследование динамики отображения $f(x) = rxe^{-x}$, $x\ in\mathbb{R}$, в зависимости от значений параметра $r \in \mathbb{R} \setminus \{0\}$. Найдены притягивающие и отталкивающие неподвижные точки, периодические орбиты с периодами степеней числа 2, изучены бифуркационные диаграммы в случаях существования бифуркаций удвоения периода, а также интервалы значений параметра, где динамика отображения имеет хаотический характер.

Результаты аналитического исследования динамики отображения $f(x)$ интерпретированы для биологической модели Рикера описания пополнения рыбных популяций. Для модели рыбной популяции должны выполняться условия $x \geq 0$ и $r > 0$. В этом случае множество значений параметра r разбивается на 3 интервала: $0 < r < 1$, $1 < r \leq e^2$, $r > e^2$.

Как показывает исследование поведения отображения, наибольший интерес представляет динамика $f(x)$ на интервале $1 < r \leq e^2$. Динамическая система находится в стационарном состоянии при $x = 0$ (отталкивающая неподвижная точка) и $x = \ln r$ (притягивающая неподвижная точка). Эти точки соответствуют замещающему уровню запаса и воспроизводства. Рассмотрим отдельно два интервала параметра r.

$1 < r < e$. Орбиты точек $x \in (0, \ln r) \cup (\ln r, +\infty)$ сходятся к неподвижной точке $x = \ln r$. Если численность родительского запаса меньше значения $\ln r$, то число рекрутов с каждым поколением возрастает, но не превысит замещающий уровень запаса и воспроизводства, равный $\ln r$. Таким образом, пополнение достигнет максимального значения при родительском запасе равном $\ln r$. Если численность родительского запаса больше значения $\ln r$, то число рекрутов с каждым поколением будет убывать до замещающего уровня равного $\ln r$.

$e < r < e^2$. Интервал $(0, +\infty)$ – бассейн притяжения неподвижной точки $x = \ln r$, где $\ln r$ – замещающий уровень запаса и воспроизводства. Максимальное значение пополнения не будет превышать r/e (при $x = 1$).

Если численность родительского запаса не превышает $\ln r$, то в течение первых нескольких поколений число рекрутов увеличивается. Но с некоторого момента число рекрутов начнет колебаться (возрастает и убывает через поколение) и приближаться к замещающему уровню. Если же численность родительского запаса больше $\ln r$, то число рекрутов уменьшается и с некоторого момента начнет приближаться к замещающему уровню (колебательно). В случае $0 < r < 1$ система находит-

ся в стационарном состоянии и неподвижные точки $x = 0$ и $x = \ln r$ соответствуют замещающему уровню запаса и воспроизводства. Родительский запас с течением времени постоянно убывает и стремится к 0. Таким образом, сокращение численности рекрутов, пополняющих промысловый запас, ведет к снижению численности популяции с каждым поколением, а, впоследствии, и к ее вымиранию. При $r > e^2$ существуют две неподвижные отталкивающие точки $x = 0$ и $x = \ln r$. А также существуют 2^n-кратные притягивающие орбиты ($n > 1$), кроме того, возможно существование хаотического поведения отображения, что подтверждают бифуркационные диаграммы.

Таким образом, самой благоприятной ситуацией для развития рыбной популяции, прогноза ее численности и хорошего улова являются значения параметра из интервала $1 < r < e^2$. В данном случае наблюдается устойчивое состояние системы, при котором величина пополнения рыбной популяции удовлетворяет требованиям промыслового улова.

DISCRETE DYNAMIC SYSTEMS IN INVESTIGATION OF POPULATION MODELS

E.N. Matveeva, N.I. Nasyrova

We investigate dynamics of the mapping $f(x) = rxe^{-x}$, $x \in \mathbb{R}$, depending on values of the parameter $r \in \mathbb{R} \setminus \{0\}$. We interpret results of analytic investigations for the biologic model by Ricker and find values of r for which the situation is most favorable for development of fish population, forecast of its size, and fishing catch.

Keywords: discrete dynamical system, biology population, Ricker model.

УДК 514.5

О СИНГУЛЯРНЫХ ИНТЕГРАЛЬНЫХ УРАВНЕНИЯХ НА СЧЕТНОМ МНОЖЕСТВЕ ЗАМКНУТЫХ НЕСПРЯМЛЯЕМЫХ КРИВЫХ

С.Р. Миронова[1], Л.Д. Погодина[2]

1 *srmironova@yandex.ru*; Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ

2 *apogodina@yandex.ru*; Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ

Для сингулярного интегрального оператора, определенного на счетном множестве кривых, получены аналоги формул Сохоцкого. Изучены вопросы эквивалентности связанного с этим оператором сингулярного уравнения и союзного с ним краевой задаче Римана на счетном множестве неспрямляемых кривых.

Ключевые слова: сингулярное интегральное уравнение, краевая задача Римана, формулы Сохоцкого.

Рассматривается характеристическое сингулярное интегральное уравнение

$$K_0\varphi \equiv a(t)\varphi(t) + b(t)S_\Gamma\varphi(t) = f(t), \quad t \in \Gamma, \tag{1}$$

и союзное с ним уравнение

$$K_0'\psi \equiv a(t)\psi(t) + b(t)S_\Gamma(b\psi)(t) = h(t), \quad t \in \Gamma, \tag{2}$$

в случае, когда контур Г состоит из счетного множества замкнутых неспрямляемых кривых Γ_k, не вложенных друг в друга и имеющих точку сгущения $z_0 \neq \infty$.

На заданные функции $a(t)$, $b(t)$, $f(t)$, $h(t)$ и искомые функции $\varphi(t)$ и $\psi(t)$ точек контура Г налагаются некоторые условия в терминах фрактальной размерности Г. Поскольку контур Г состоит из неспрямляемых кривых, сингулярный интегральный оператор S_Γ понимается в обобщенном смысле.

В работе получены аналоги формул Сохоцкого для этого оператора и изучены вопросы эквивалентности сингулярных уравнений (1) и (2) краевой задаче Римана на счетном множестве неспрямляемых кривых.

Литература

1. Миронова С. Р. *Сингулярные интегральные уравнения на счетном множестве замкнутых неспрямляемых и фрактальных кривых* // Изв. вузов. Математика. – 1998. – No 5. – С. 43–49.

SINGULAR INTEGRAL EQUATION ON A COUNTABLE SET
OF CLOSED NON-RECTIFIABLE CURVES

S.R. Mironova, A.Yu. Pogodina

We obtaine analogs of Sochocki's formulas for an singular integral equation for a countable set of non-rectifiable curves. We also investigate equivalence of the singular integral equation, associated with the operator, and its conjugate to some Riemann boundary value problems.

Keywords: singular integral equation, Riemann boundary value problem, Sochocki formulas.

УДК 517.55

ФОРМУЛА ДЛЯ ВЫЧЕТНОГО ИНТЕГРАЛА, СВЯЗАННОГО С СИСТЕМОЙ НЕАЛГЕБРАИЧЕСКИХ УРАВНЕНИЙ

Е.К. Мышкина[1]

1 *elfifenok@mail.ru*; Сибирский федеральный университет, Институт математики и фундаментальной информатики

В данной статье рассматриваются неалгебраические системы уравнений общего вида. Определяются вычетные интегралы по циклам, связанным с системой. Приведены формулы для их вычисления и установлена их связь со степенными суммами корней системы.

Ключевые слова: неалгебраические системы уравнений, вычетные интегралы, степенные суммы корней.

Рассмотрим систему уравнений вида

$$f_i(z_1,\dots,z_n) = P_i(z_1,\dots,z_n) + Q_i(z_1,\dots,z_n), \quad i = 1,2,\dots,n \tag{1}$$

где P_i — младшая однородная часть разложения Тейлора функции $f_i(z)$. Степень всех мономов, входящих в P_i, равна m_i. В функциях Q_i степени всех мономов строго больше чем m_i.

В дальнейшем будем предполагать, что система многочленов $P_1(z),\dots,P_n(z)$ – невырождена, т.е. ее общим нулем служит точка 0 – начало координат.

$$Q_i(z) = \sum_{\|\alpha\|>m_i} a^i_\alpha z^\alpha, \tag{2}$$

$$P_i(z) = \sum_{\|\beta\|=m_i} b^i_\beta z^\beta, \tag{3}$$

где $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\alpha_j \geqslant 0$, $\alpha_j \in \mathbb{Z}$, а $z^\alpha = z_1^{\alpha_1} \cdot z_2^{\alpha_2} \cdots z_n^{\alpha_n}$; $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$, $\beta_j \in \mathbb{N}$, $\|\beta_i\| = \beta^i_1 + \beta^i_2 + \ldots + \beta^i_n = m_i$, а $z^\beta = z_1^{\beta_1} \cdot z_2^{\beta_2} \cdots z_n^{\beta_n} \quad i = 1, 2, \ldots, n$.

Обозначим через Γ_P цикл

$$\Gamma_P = \{z \in \mathbb{C}^n : |P_i| = r_i, \quad r_i > 0, \ i = \overline{1, n}\}. \tag{4}$$

Этот цикл является компактом в силу того, что система $P_i(z) = 0$ имеет только одно решение – точку 0 (невырожденная).

Обозначим через J_γ вычетный интеграл

$$J_\gamma = \frac{1}{(2\pi\sqrt{-1})^n} \int\limits_{\Gamma_P} \frac{1}{z^\gamma} \cdot \frac{df}{f} = \tag{5}$$

$$= \frac{1}{(2\pi\sqrt{-1})^n} \int\limits_{\Gamma_P} \frac{1}{z_1^{\gamma_1} \cdot z_2^{\gamma_2} \cdots z_n^{\gamma_n}} \cdot \frac{df_1}{f_1} \wedge \frac{df_2}{f_2} \wedge \ldots \wedge \frac{df_n}{f_n},$$

где $\gamma = (\gamma_1, \ldots \gamma_n)$ — мультииндекс.

Теорема 1. *При сделанных предположениях для функций f_i вида (1) справедливы формулы:*

$$J_\gamma = \frac{1}{(2\pi\sqrt{-1})^n} \int\limits_{\Gamma_P} \frac{1}{z^{\gamma+I}} \cdot \frac{df}{f} =$$

$$= \frac{1}{(2\pi\sqrt{-1})^n} \sum_{\|\alpha\| \leqslant \|\gamma\|+n} (-1)^{\|\alpha\|} \int\limits_{\Gamma_P} \left[\frac{\Delta \cdot Q^\alpha}{z^{\gamma+I} \cdot P^{\alpha+I}} \right],$$

где $\alpha = (\alpha_1, \ldots, \alpha_n)$ — мультииндекс, Δ — якобиан системы, $z^\gamma = z_1^{\gamma_1} \cdot \ldots \cdot z_n^{\gamma_n}$, $Q^\alpha = Q_1^{\alpha_1} \cdot \ldots \cdot Q_n^{\alpha_n}$, $P^{\alpha+I} = P_1^{\alpha_1+1} \cdot \ldots \cdot P_n^{\alpha_n+1}$,

Предположим теперь, что $Q_i(z)$ — многочлены вида

$$Q_i(z) = \sum_{\|\alpha\|>m_i} C^i_\alpha z^\alpha \quad i = 1, 2, \ldots, n, \tag{6}$$

где α — мультииндекс, $z^\alpha = z_1^{\alpha_1} \cdot \ldots \cdot z_n^{\alpha_n}$. Для каждого i-ого уравнения выполнено условие, что

$$\deg_{z_i} P_i < \deg_{z_i} Q_i, \quad \deg_{z_1 \ldots [z_i] \ldots z_n} P_i \geq ord_{z_1 \ldots [z_i] \ldots z_n} Q_i.$$

Пусть $\deg P_i = m_i$, $\quad \deg Q_i = s_i$. Тогда $\deg_{z_i} P_i = m^i_i$, $\quad ord_{z_i} Q_i = s^i_i$,

Делая замену в системе (1) $z_i = \dfrac{1}{w_i}$, предполагая, что все $w_j \neq 0$, $i = \overline{1, n}$, получаем

$$\widetilde{f}_i(w) = \widetilde{P}_i(w) + \widetilde{Q}_i(w), \tag{7}$$

где функции

$$\widetilde{Q}_i(w_1,\dots,w_n) = w_1^{m_i^1-s_i^1}\cdot\ldots\cdot[w_i]\cdot\ldots\cdot w_n^{m_i^n-s_i^n}\cdot\sum_{\|\alpha\|>0} a_\alpha^i w_1^{m_i^1-\alpha_i^1}\cdot\ldots\cdot w_n^{m_i^n-\alpha_i^n}$$

при чем $\deg Q_i = s_i,\quad \deg\widetilde{P}_i > \deg\widetilde{Q}_i,\ i=\overline{1,n}.$

Обозначим через $\widetilde{\Gamma}_P$ цикл

$$\widetilde{\Gamma}_P = \{w\in\mathbb{C}^n : |\widetilde{P}_i| = \epsilon_i,\quad \epsilon_i>0,\ i=\overline{1,n}\}. \tag{8}$$

Лемма 1. *Для произвольного мультииндекса γ интеграл J_γ равен*

$$J_\gamma = \frac{1}{(2\pi\sqrt{-1})^n}\int\limits_{\widetilde{\Gamma}_P} w_1^{\gamma_1}\cdot w_2^{\gamma_2}\cdots w_n^{\gamma_n}\cdot\frac{d\widetilde{f}_1}{\widetilde{f}_1}\wedge\frac{d\widetilde{f}_2}{\widetilde{f}_2}\wedge\ldots\wedge\frac{d\widetilde{f}_n}{\widetilde{f}_n} \tag{8}$$

Лемма 2. *Пусть $w_{(1)},\dots,w_{(s)}$ — корни системы (7) (с учетом их кратностей), где $w_{(j)} = (w_{(j1)}, w_{(j2)},\dots,w_{(jn)})$, $j=1,2,\dots,s$. Тогда*

$$J_\gamma = \sum_{j=1}^{s} w_{(j1)}^{\gamma_1+1}, w_{(j2)}^{\gamma_2+1},\dots, w_{(jn)}^{\gamma_n+1}.$$

Теорема 2. *Справедливо равенство*

$$\sum_{j=1}^{p}\frac{1}{z_{j1}^{\gamma_1+1}\cdot z_{j2}^{\gamma_2+1}\cdot\ldots\cdot z_{jn}^{\gamma_n+1}} =$$

$$= \sum_{\|\alpha\|\leqslant\|\gamma\|+n}(-1)^{\|\alpha\|}\int\limits_{\widetilde{\Gamma}_P}\left[\widetilde{\Delta}\cdot w^{\gamma+I}\frac{\widetilde{Q}^\alpha}{\widetilde{P}^{\alpha+I}}\right]dw,$$

где $\widetilde{\Delta}$ – якобиан системы (7).

Работа выполнена при финансовой поддержке РФФИ (проект 15-01-00277, 16-31-00173), программы Президента “Ведущие научные школы РФ” (проект № НШ-9149.2016.1).

Литература

1. Кытманов А. М., Мышкина Е. К. *О вычислении степенных сумм корней одного класса систем неалгебраических уравнений* // Сиб. электр. матем. изв. – 2015 – Т. 12. – С. 190–209.

2. Kytmanov A. A., Kytmanov A. M., Myshkina E. K. *Finding residue integrals for systems of non-algebraic equations in $\mathbb{C}^n$* // Journal of Symbolic Computation. –2015. – V. 66. – P. 98–110.

RESIDUE INTEGRAL FORMULA FOR A CLASS OF SYSTEMS OF NON-ALGEBRAIC EQUATIONS

E.K. Myshkina

This article discusses systems of non-algebraic equations of a general form. We define residue integrals over the cycles associated to the system. Formulas for their computation and relation to power sums of the roots of a system are given.

Keywords: non-algebraic system of equations, residue integrals, power sums of roots.

УДК 519.6

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ВИЗУАЛИЗАЦИИ ДАННЫХ СРЕДСТВАМИ ЯЗЫКА PROCESSING

А.И. Немкова[1]

1 *nemkovaaiv@stud.kpfu.ru*; Казанский (Приволжский) федеральный университет, Институт математики и механики им. Н.И. Лобачевского

В данной статье мы исследуем возможности использования открытого языка программирования Processing в образовании: непосредственно в учебном процессе при изучении языков программирования и различных платформ.

Ключевые слова: процессинг, язык Processing, Processing в образовании, язык программирования, визуализация.

Компьютерные технологии постоянно совершенствуются: разрабатываются новые платформы для доступного освоения языков программирования, с простым синтаксисом и богатыми возможностями создания насыщенных графических и интерактивных программ. В качестве одного из способов работы с большими данными и решением проблемы сложности их восприятия выступает визуализация данных.

Processing – это средство создания законченных профессиональных работ: изображений, видео, интерактивных инсталляций, приложений. Язык Processing синтаксически базируется на языке Java. Создателями данного языка являются Кэйси Риз и Бэн Фрай. Он был создан в 2001 году в Массачусетском Технологическом Институте (MIT) и в наше время активно развивается некомерческой инициативной группой (Processing Foundation, processing.org). Изначально этот язык был разработан с целью обучения школьников, для мотивации к программированию. Далее Processing был значительно расширен добавлением в него визуальных возможностей. Кроме того, его стали использовать художники-дизайнеры и архитекторы для создания своих проектов. Такие компании как New York Times, General Electric, Nokia, Yahoo! стали использовать Processing для визуализации своих внутренних данных [1].

Отличительные особенности языка Processing

Существует широкий спектр языков, ориентируемых на эстетичные объекты, а не на исполняемый код: графические изображения, демонстрационные ролики или WEB сайты. К специализированным языкам такого рода относится POV-Ray, позволяющий создавать трехмерные изображения с использованием техники рендеринга; TeX, компилирующий текст в макеты, готовые для тиражирования типографии; SVG (Scalable Vector Graphics) – схема XML для создания векторной графики, и так далее. Также существуют другие, более общие языки: ActionScript лежит в основе Macromedia Flash и широко распространён в Web. В дальнем конце спектра находятся языки общего назначения, такие как C, Java, Perl и Python – языки, которые позволяют использовать все возможности компьютера. Processing можно отнести как к чему-то среднему. С одной стороны, он является языком программирования

общего назначения (позволяет вызывать любые функции Java), но при этом он ограничивается очень небольшим набором упрощённых объектов – точки, сферы, прямоугольники – и несложной моделью трехмерного пространства. Код этого языка компилируется в интерактивный графический элемент.

Структура программы

Программа на Processing называется скетч (от англ. sketch — эскиз). Каждый скетч в Processing является классом, наследуемым от Java-класса PApplet, который содержит в себе большинство возможностей языка Processing. Перед выполнением скетча он преобразуется в код на языке Java для выполнения в среде Windows/Linux/MacOS/Android либо в Javascript-код для выполнения в браузере внутри Canvas. При программировании на языке Processing все создаваемые классы являются внутренними классами основного. Это накладывает определённые ограничения при разработке. Несмотря на то, что Processing и очень простой язык, который допускает много вольностей, для того, чтобы написать достойную программу необходимо следовать некоторым соглашениям.

Например, все функции инициализации: size() – размер окна, stroke() – цвет линий, background() – цвет фона, и некоторые другие необходимо помещать внутрь специальной служебной функции void setup() [6].

Следующая служебная функция – void draw(). Её аналогом можно назвать int main() в C++. Эта функция является основой для построения любой анимации. Её особенностью является то, что она автоматически вызывается при каждом обновлении фреймбуфера.

Последнее соглашение связано с позиционированием объектов в координатной плоскости. После инициализации размера окна функцией setup(), внутри программы становятся доступны две глобальных константы — WIDTH и HEIGHT, в которых хранится соответственно ширина и высота окна. Каждый раз, когда вы хотите разместить, скажем, круг по центру экрана, необходимо пользоваться такой записью [2].

Пример программы с использованием соглашений

Команда variableEllipse() вычисляет скорость движения мыши, рисует небольшой эллипс, если мышь медленно движется или изображает большой эллипс, если мышь быстро движется. С помощью команды random() мы случайным образом определяем заливку эллипсов.

```
void setup() {
size(640, 360);
  float r= random(225);
  float a = random(255);
  float b = random(255);
  color c= color(r, a, b);
  background(c);}

void draw()
{ variableEllipse(mouseX, mouseY, pmouseX, pmouseY);}

void variableEllipse(int x, int y, int px, int py) {
  float speed = abs(x-px) + abs(y-py);
  stroke(speed);
  ellipse(x, y, speed, speed);
  fill(random(255),random(255),random(255));}
```

Рис. 1. Эскиз программы рисования случайно выбранными кругами в Processing

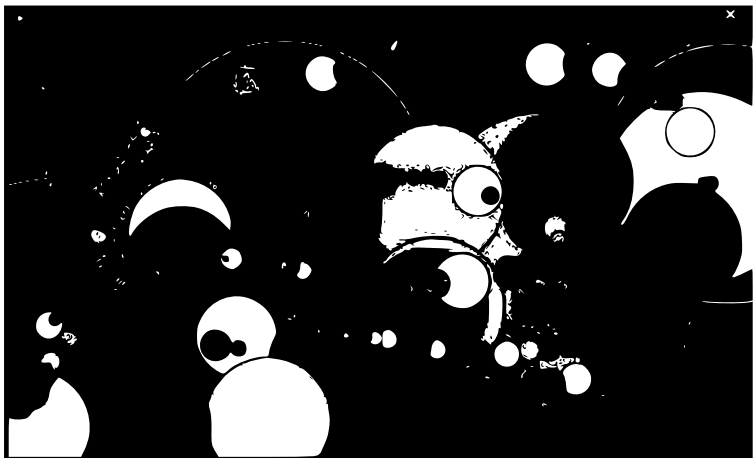


Рис. 2. Рисование случайно выбранными кругами в Processing

Возможности визуализации данных средствами языка processing

На базе Processing был создан язык Wiring для довольно популярной платформы Arduino, получившей огромную известность в любительской робототехнике. Если скачать и запустить Processing Development Evironment, то можно обнаружить его абсолютное сходство с Arduino IDE. Из Processing-а можно общаться с Arduino, при помощи протокола Firmata, что открывает широкие возможности для изучении основ робототехники.

Сегодня Processing так же легко запускается на мобильной платформе Android. Большое пространство для экспериментов со свободными SDK и эмуляторами, но гораздо интереснее поработать непосредственно с устройством. Используя свободное ПО, вы можете делать скетчи на мобильной платформе. Программирование для Android или processing выполняет все те же основные функции, что и Processing для десктопа – 2D и 3D визуализацию; манипулирование данными, изображениями и типами – кроме того, можно использовать в коде вызов стандартных API-функций Android прямо в проекте.

Существует возможность создавать 3D-аппликации (в том числе и игры), так

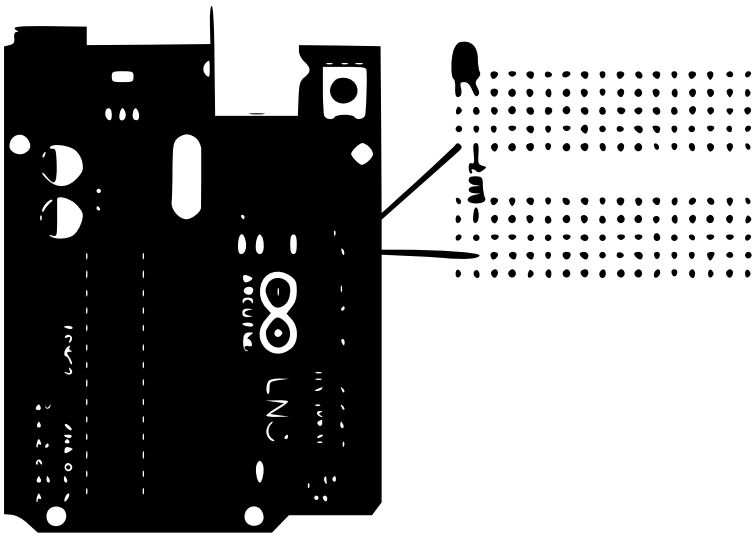


Рис. 3. Платформа Arduino

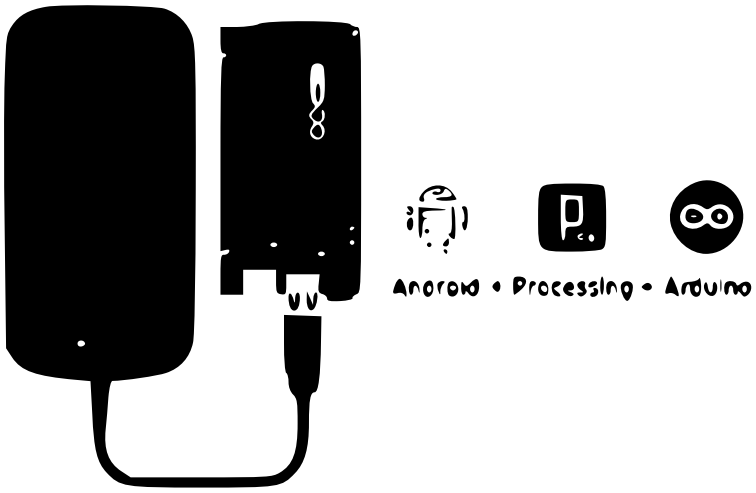


Рис. 4. Управление Arduino с помощью Android

как Processing имеет средства поддержки OpenGL. Все эти возможности, в совокупности с большим количеством функций и очень логичным синтаксисом, делают этот язык идеальным для обучения и прививания интереса к программированию.

Литература

1. *Волшебное программирование*. URL: http://www.programmingforkids.ru/2013/09/Processing-istoriya-i-preimushestva.html

2. *Знакомство с Processing 1.0*. URL: http://ru.wikipedia.org/wiki/

3. *Processing*. – Материал из Википедии — свободной энциклопедии. URL: http://ru.wikipedia.org/wiki/Processing

4. *Processing и Arduino*. URL: http://robocraft.ru/blog/arduino/336.html

5. *Руководство по использованию Processing под Android*. URL: http://www.malbred.com/soft-po-vidzheingu/rukovodstvo-po-ispolzovaniyu-processing-pod-android.html

6. *Знакомство с Processing 1.0*. URL: https://habrahabr.ru/post/58314/

7. Вантомм Я. *Processing 2: креативное программирование.* – Packt Publishing Ltd., 2012. – 292 с.

EXPLORING THE POSSIBILITIES OF VISUALIZING DATA USING LANGUAGE PROCESSINGE

A.I. Nemkova

In this article, we explore the possibilities of using the open programming language «Processing» in education: directly in learning programming languages and various platforms.

Keywords: Processing, Processing language in education, programming language, visualization, exploring of visualizing.

УДК 372.851

УЧЕБНО-ПОЗНАВАТЕЛЬНЫЕ ЗАДАЧИ КАК СРЕДСТВО РАЗВИТИЯ ЛОГИЧЕСКИХ УУД ПРИ ОБУЧЕНИИ МАТЕМАТИКИ В 5-7 КЛАССАХ

Л.И. Нуркаева[1], Е.Р. Садыкова[2]

1 *nurkaeva.liana@yandex.ru*; МБОУ «Пестречинская СОШ №1 с углублённым изучением отдельных предметов»

2 *sadikova-er@mail.ru*; Казанский (Приволжский) федеральный университет

В статье рассматриваются учебно-познавательные задачи как средство развития логических универсальных учебных действий при обучении математике в 5-7 классах.

Ключевые слова: обучение математике, учебно-познавательные задачи, логические универсальные учебные действия.

Совершенствование современного образования в последнее время в значительной степени связано с инновационными подходами в подготовке учащихся. Сложившаяся ситуация ставит перед школой важную задачу – формирование личности, способной к эффективной и продуктивной деятельности, готовой осуществлять быстрый поиск решений в различных социально-значимых ситуациях.

Федеральный государственный образовательный стандарт (стандарт второго поколения) подразумевает под собой совокупность требований, обязательных при реализации основной образовательной программы среднего общего образования. Требования к результатам освоения основной образовательной программы, ее структуре и условиям реализации учитывают возрастные и индивидуальные особенности обучающихся при получении среднего общего образования, а также значимость данного уровня общего образования для продолжения обучения в организациях, осуществляющих образовательную деятельность, профессиональной деятельности и успешной социализации [3].

В основе федерального государственного образовательного стандарта лежит личностно-деятельностный подход. В отличие от ранее принятых стандартов, где главным было получение базовых знаний, так называемых знаний, умений и навыков, в стандарте второго поколения приоритетным является личность ученика и её развитие. А развитие личности, согласно ФГОС, происходит посредством развития универсальных учебных действий (УУД), которые выступают в качестве метапредметных и личностных результатов обучения.

Универсальные учебные действия – это способность ученика учиться, способность ученика самосовершенствоваться, самостоятельно открывать новые знания, формировать компетентности. Иными словами, ученик сам проектирует для себя процесс получения знаний, является архитектором учебного процесса и тем самым происходит социализация ребёнка и подготовка его к жизни в современном мире.

Главной функцией УУД является создание условия и обеспечение возможностей для самостоятельной реализации учеником процесса обучения, в том числе постановки целей, поиск учебных средств и методов достижения поставленной цели, анализ, оценка и коррекция полученных результатов [3].

Среди универсальных учебных действий выделяют логические действия. Данные действия имеют наиболее общий характер и направлены на установление связей и отношений в любой области знания. В рамках школьного обучения под логическим мышлением подразумевают способность и умение учащихся производить простые логические действия такие, как анализ, синтез, сравнение и др., а также составные логические операции (построение утверждения, опровержения и отрицания с использованием дедуктивных и индуктивных логических схем). В классификации логических действий выделяют: сравнение конкретно-чувственных и иных данных с целью выделения тождества, различия, определения общих признаков и составления классификации; опознание конкретно-чувственных и иных объектов с целью их включения в тот или иной.

Именно в математике логические формы и отношения проявляются в явной форме как предмет усвоения учащимися. Логические действия, выступая инструментальным базисом математики, позволяют также упорядочить и систематизировать имеющиеся математические знания, вывести и конструировать новые знания. Уроки математики – это «мастерская», где учителю предоставляется возможность обучить детей искусству решения задач, вместе с тем формируя у них особый склад ума, позволяющий видеть закономерности, проводить наблюдения, сравнивать и выдвигать свои догадки и гипотезы.

Анализ психолого-педагогической, методической литературы показал, что одним из средств формирования и развития логических универсальных учебных действий является использование учебно-познавательных задач. Учебно-познавательные задачи позволяют учащимся усвоить математические понятия, повышают их вычислительную культуру, способствуют более полной реализации межпредметных связей, развивают у учащихся способность анализировать, рассуждать, обосновывать, доказывать, отстаивать свою точку зрения, развивают логическое мышление, познавательные способности через усвоение способов решения задач, учат применению метода познания действительности – моделированию. Как показало исследование, на уроках математики в 5-7 классах можно предлагать учащимся задачи на развитие логических учебных универсальных действий следующих типов:

1. *Проблемная задача.*

   Сравнить дроби: $\frac{1}{2}$ и $\frac{2}{3}$.

   Данная задача предлагается учащимся перед введением темы «Приведение дробей с разными знаменателями к общему знаменателю» и «Сравнение дробей с разными знаменателями». Учащиеся, оценивая эти две дроби и сравнивая

их с половиной, приходят к выводу, что первая дробь меньше второй.

2. *Ситуационная задача.* «Экономный путешественник»

   Много ли существует вариантов добраться из Казани в Самару? Экономный путешественник никак не может решить, на чём ему отправиться из Казани в Самару: на поезде или на машине. Помоги путешественнику определиться. С помощью атласов автомобильных и железных дорог рассчитай расстояние от одного города до другого и время, которое затратит пассажир, если скорость поезда 80 км/ч, а скорость автобуса 60 км/ч. Цена билета на поезд равна 731 руб, а на автобус 800 руб. Каким способом выгоднее добраться?

   Ситуационные задачи помогают выявлять ключевые проблемы; искать альтернативные пути решения и оценивать их; выбирать оптимальное решение и формировать программы действий и т. п. [2].

3. *Текстовые сюжетные задачи.* Автобус перевозил туристов из долины на горнолыжный курорт. Первые 3 часа автобус двигался со скоростью 80 км/ч, затем еще 3 часа со скоростью 40 км/ч и последние 4 часа со скоростью 30 км/ч.

   а) Найдите среднюю скорость движения автобуса на всем пути.

   б) Почему автобус вынужден был менять скорость движения? Какие горнолыжные курорты известны? Где они находятся?

   Стандартная сюжетная задача по теме «Среднее арифметическое». Задача требует простого воспроизведения имеющихся знаний. Учащиеся, применяя правило или образец, самостоятельно решают задачу.

4. *Задачи с избытком информации.*

   В школе 1800 учащихся. Среди них 680 мальчиков и 1120 девочек. В среду на уроках отсутствовало 120 учеников. Какая часть учащихся школы была в этот день на уроках? [1]

5. *Задачи с недостатком информации.*

   Найдите $\angle DCE$, если $\angle FCE$ равен 56° [1].

6. *Задание на формирование умения поиска ответа.*
   По ответу нужно догадаться, о чём спросили.
   Учитель: - “Сумма длин всех сторон”.
   Ученик: - “Что такое периметр?”
   Учитель: - “Первую дробь умножить на дробь, обратную второй”.
   Ученик: - “Деление дробей”.

7. *Задачи, основанные на работе с учебником*

   - Проанализировать заголовок и выдвинуть предположения о содержании параграфа.
   - На основании имеющихся примеров в параграфе придумать свои примеры.
   - Составить схемы, рисунки, чертежи по имеющейся информации (опорный конспект по теме).

- Запомнить материал, используя приемы запоминания (пересказ по схеме, мнемонические приемы).
- Придумать вопросы по тексту и задать их соседу по парте, учителю.

В настоящее время авторами проводится опытно-экспериментальная работа по развитию учебных логических действий с использованием учебно-познавательных задач. В исследовании принимают участие ученики шестых классов (54 ученика) Пестречинской СОШ №1 РТ. Диагностическое обследование показало, что на первом этапе экспериментальной работы у большинства учащихся слабо выражены логические действия. Ученики не умеют анализировать, обобщать, сопоставлять данные. Все это говорит о низком уровне сформированности универсальных действий, поэтому продолжается работа по развитию логических действий с использованием учебно-познавательных задач.

Литература

1. Дорофеев Г. В., Суворова С. Б., Бунимович Е. А. *Математика. 7 класс. ФГОС.* – М.: Просвещение, 2017. – 286 с.

2. Суровцева В. А. *Ситуационная задача как один из современных методических ресурсов обновления содержания школьного образования* // Школьная педагогика. – 2016. – № 4. – С. 48–57.

3. *Федеральный государственный образовательный стандарт среднего (полного) общего образования.* – М.: Просвещение, 2014. – 63 с.

EDUCATIONAL OBJECTIVES AS A TOOL OF DEVELOPING LOGICAL UNIVERSAL EDUCATIONAL ACTIVITIES IN TEACHING OF MATHEMATICS IN GRADES 5-7

L.I. Nurkaeva, E.R. Sadykova

This article describes the educational objectives as a tool of developing logical universal educational activities in teaching mathematics in grades 5-7.

Keywords: educational objectives, logical universal educational activities.

УДК 514.763.7+512.5

ТРИ-ТКАНИ БОЛА С КОВАРИАНТНО ПОСТОЯННЫМ ТЕНЗОРОМ КРИВИЗНЫ

Е.А. Оноприенко[1], А.М. Шелехов[2]

1 *katrinonoprienko@mail.ru*; Московский педагогический государственный университет
2 *amshelekhov@rambler.ru*; Московский педагогический государственный университет

Рассматриваются инфинитезимальные свойства многомерных средних три-тканей Бола с ковариантно постоянным тензором кривизны (ткани $B_m^{\triangledown}$); заложены основы классификации таких тканей по рангу тензора кручения. Для три-ткани $B_m^{\triangledown}$ ранга ρ методом Картана построен адаптированный репер и найдена соответствующая система структурных (дифференциальных) уравнений. Доказывается, что три-ткань $B_m^{\triangledown}$ ранга ρ несет нормальную подткань, которая является групповой, причем соответствующая фактор-ткань является регулярной три-тканью. Путем интегрирования структурных уравнений найдены новые семейства примеров многомерных тритканей специального типа и гладких луп Бола, являющихся обобщение полупрямого

произведения двух абелевых групп Ли.

Ключевые слова: многомерная три-ткань, три-ткань Бола, групповая три-ткань, эластичная три-ткань, G-ткань, гладкая лупа Бола.

Три-тканью называется совокупность трех попарно трансверсальных гладких слоений коразмерности r на гладком многообразии M размерности $2r$. Локально слоения всегда можно задать уравнениями $x^i = \text{const}$, $y^i = \text{const}$ и $f^i(x^j, y^k) = \text{const}$; здесь и далее $i, j, k, \ldots = 1, 2, \ldots, r$. Локально три-ткань вполне определяется уравнением $z = f(x, y)$, которое связывает параметры x, y, z слоев первого, второго и третьего слоений, проходящих через одну точку, и называется уравнением три-ткани. В силу трансверсальности слоев уравнение три-ткани разрешимо (локально) относительно переменных x и y, поэтому оно определяет гладкую локальную квазигруппу, которая называется координатной квазигруппой три-ткани W. Следуя В. Бляшке, мы рассматриваем три-ткани с точностью до локальных диффеоморфизмов.

Систематическое изучение многомерных три-тканей положено работой Черна [1]. Используя подход Картана-Лаптева, М.А. Акивис создал эффективный метод для изучения многомерных три-тканей. Этим методом получены все существенные результаты по теории многомерных три-тканей, см. [2].

Средние ткани Бола (ткани B_m) занимают особое место в теории тканей. Их алгебраический аналог — многомерные гладкие лупы Бола — следующие после аналитических луп Муфанг по близости своих свойств к группам Ли. Три-ткани B_m: 1) обладают замкнутой G-структурой класса 3 — ковариантные производные тензора кривизны являются комитантами тензоров кручения и кривизны; 2) на третьем слоении этих тканей естественным образом возникает структура симметрического пространства. Эта симметрия обладает специальными свойствами, которые изучались многими авторами.

Три-ткани B_m были введены Г. Болом в [3]. Их алгебраические свойства исследовались В.Д. Белоусовым и другими авторами. Четырехмерные ткани Бола полностью описал А.Д. Иванов. Ткани B_m произвольной размерности исследовала В.И. Федорова, которая, в частности, заложила основы классификации шестимерных тканей B_m. Специальный класс тканей Бола — эластичные ткани или ткани E — исследовались А. М. Шелеховым, Г. Баландиной, К.Р. Джукашевым. Три-ткани B_m с тензором кривизны минимального ранга рассматривались М. И. Антиповой. Гладкие лупы Бола исследовались Л.В. Сабининым и П.О. Михеевым.

Доказаны следующие утверждения.

1. Пусть кобазис дифференциальных форм $\underset{1}{\omega}{}^i$ и $\underset{2}{\omega}{}^i$ $(i, j, k, \ldots = 1, \ldots, r)$ на многообразии M выбран так, что формы $\underset{1}{\omega}{}^i$, $\underset{2}{\omega}{}^i$ и $\underset{1}{\omega}{}^i + \underset{2}{\omega}{}^i$ аннулируются соответственно на 1-ом, 2-ом и 3-ем слоениях ткани $B_m^{\triangledown}$. Тогда эти формы удовлетворяют системе дифференциальных уравнений

$$\begin{gathered} d\underset{1}{\omega}{}^i = \underset{1}{\omega}{}^j \wedge \omega_j^i + a_{jk}^i \underset{1}{\omega}{}^j \wedge \underset{1}{\omega}{}^k, \quad d\underset{2}{\omega}{}^i = \underset{2}{\omega}{}^j \wedge \omega_j^i - a_{jk}^i \underset{2}{\omega}{}^j \wedge \underset{2}{\omega}{}^k, \\ d\omega_j^i = \omega_j^k \wedge \omega_k^i + b_{jkl}^i \underset{1}{\omega}{}^k \wedge \underset{2}{\omega}{}^l, \end{gathered} \tag{1}$$

$$\nabla a_{jk}^i = -b_{[jk]\ell}^i \left(\underset{1}{\omega}{}^\ell - \underset{2}{\omega}{}^\ell \right), \quad \nabla b_{jk\ell}^i = 0, \tag{2}$$

замкнутой относительно операции внешнего дифференцирования в силу соотношений

$$\begin{aligned} &b^i_{[jk\ell]} = 2a^m_{[jk}a^i_{|m|\ell]}, \quad b^i_{j(kl)} = 0, \quad b^i_{jkp}a^p_{\ell m} = 0, \\ &a^p_{jk}b^i_{p\ell m} = a^i_{pk}b^p_{j\ell m} + a^i_{jp}b^p_{k\ell m}, \quad b^i_{jkp}b^p_{lmq} = 0, \quad b^i_{prs}b^p_{jkl} = b^i_{pkl}b^p_{jrs}. \end{aligned} \tag{3}$$

Здесь a^i_{jk} — тензор кручения, b^i_{jkl} — тензор кривизны.

2. Негрупповых четырехмерных тканей $B^{\triangledown}_m$ не существует.

3. Класс негрупповых шестимерных тканей $B^{\triangledown}_m$ содержит только две три-ткани — это известные эластичные ткани E_1 и E_2.

Пусть $\mathscr{A}$ — алгебра, определяемая тензором кручения. Назовем рангом тензора кручения размерность производной алгебры $\mathscr{A}'$.

4. Ткани $B^{\triangledown}_m$ с тензором кручения ранга 0, r или $r-1$ являются групповыми тканями.

Анализ системы (1)-(3) приводит к следующей теореме.

5. Класс тканей $B^{\triangledown}_m$ с тензором кручения ранга 1 совпадает с классом эластичных тканей E^r_1.

(Уравнения ткани E^r_1 в локальных координатах имеют вид:

$$z^1 = x^1 + e^{2a_{\hat{k}}x^{\hat{k}}}(y^1 + \lambda_{\hat{j}\hat{k}}x^{\hat{j}}y^{\hat{k}}),\ z^{\hat{i}} = x^{\hat{i}} + y^{\hat{i}},$$

где $\hat{i},\hat{j},\hat{k} = 2,\dots,r$, $a_{\hat{k}}$ и $\lambda_{\hat{j}\hat{k}}$ — постоянные, причем $\lambda_{\hat{j}\hat{k}} = -\lambda_{\hat{k}\hat{j}}$.)

6. Для ткани $B^{\triangledown}_m$ ранга ρ существует адаптированный репер, в котором структурные уравнения этой ткани имеют вид

$$\begin{aligned} &d\underset{1}{\omega}{}^a = \underset{1}{\omega}{}^b \wedge \omega^a_b + \underset{1}{\omega}{}^v \wedge \omega^a_v + a^a_{jk}\,\underset{1}{\omega}{}^j \wedge \underset{1}{\omega}{}^k, \\ &d\underset{2}{\omega}{}^a = \underset{2}{\omega}{}^b \wedge \omega^a_b + \underset{2}{\omega}{}^v \wedge \omega^a_v - a^a_{jk}\,\underset{2}{\omega}{}^j \wedge \underset{2}{\omega}{}^k, \\ &d\underset{1}{\omega}{}^u = 0, \\ &d\underset{2}{\omega}{}^u = 0, \\ &d\omega^a_b = \omega^c_b \wedge \omega^a_c + 2(a^c_{wz}a^a_{cb} + a^c_{zb}a^a_{cw} + a^c_{bw}a^a_{cz})\,\underset{1}{\omega}{}^w \wedge \underset{2}{\omega}{}^z, \\ &d\omega^a_u = \omega^c_u \wedge \omega^a_c + b^a_{uwz}\,\underset{1}{\omega}{}^w \wedge \underset{2}{\omega}{}^z, \end{aligned} \tag{4}$$

причем ненулевые компоненты тензоров кручения и кривизны связаны соотношениями

$$\begin{aligned} &a^b_{de}a^a_{bc} + a^b_{ec}a^a_{bd} + a^b_{cd}a^a_{be} = 0,\ a^b_{du}a^a_{bc} + a^b_{uc}a^a_{bd} + a^b_{cd}a^a_{bu} = 0; \\ &a^f_{bu}(a^a_{fd}a^b_{vc} + a^a_{cf}a^b_{vd} - a^b_{cd}a^a_{fv}) + a^f_{bv}(a^a_{fd}a^b_{cu} + a^a_{cf}a^b_{du} - a^b_{cd}a^a_{fu}) = 0; \\ &(a^d_{uv}a^a_{db} + a^d_{vb}a^a_{du} + a^d_{bu}a^a_{dv})(a^e_{wz}a^b_{ec} + a^e_{zc}a^b_{ew} + a^e_{cw}a^b_{ez}) = \\ =&(a^d_{wz}a^a_{db} + a^d_{zb}a^a_{dw} + a^d_{bw}a^a_{dz})(a^e_{uv}a^b_{ec} + a^e_{vc}a^b_{eu} + a^e_{cu}a^b_{ev}); \\ &b^a_{buv} = 2(a^c_{uv}a^a_{cb} + a^c_{vb}a^a_{cu} + a^c_{bu}a^a_{cv}); \\ &b^a_{uvw} + b^a_{vwu} + b^a_{wuv} = 2(a^b_{uv}a^a_{bw} + a^b_{vw}a^a_{bu} + a^b_{wu}a^a_{bv}); \end{aligned}$$

$$a^a_{cb}b^b_{wuv} = 2a^b_{cw}(a^f_{uv}a^a_{fb} + a^f_{vb}a^a_{fu} + a^f_{bu}a^a_{fv}) - 2a^a_{bw}(a^f_{uv}a^b_{fc} + a^f_{vc}a^b_{fu} + a^f_{cu}a^b_{fv});$$

$$a^a_{bz}b^b_{wuv} + a^a_{wb}b^b_{zuv} = 2a^b_{wz}(a^c_{uv}a^a_{cb} + a^c_{vb}a^a_{cu} + a^c_{bu}a^a_{cv});$$

$$\begin{aligned} &b^b_{qwz}(a^c_{vb}a^a_{cu} + a^c_{bu}a^a_{cv}) - b^b_{quv}(a^c_{zb}a^a_{cw} + a^c_{bw}a^a_{cz}) = \\ =&2a^c_{wz}[a^b_{cq}(a^f_{uv}a^a_{fb} + a^f_{vb}a^a_{fu} + a^f_{bu}a^a_{fv}) - a^a_{bq}(a^f_{uv}a^b_{fc} + a^f_{vc}a^b_{fu} + a^f_{cu}a^b_{fv})] - \\ -&2a^c_{uv}[a^b_{cq}(a^f_{wz}a^a_{fb} + a^f_{zb}a^a_{fw} + a^f_{bw}a^a_{fz}) - a^a_{bq}(a^f_{wz}a^b_{fc} + a^f_{zc}a^b_{fw} + a^f_{cw}a^b_{fz})] \end{aligned}$$

и удовлетворяют дифференциальным уравнениям

$$\nabla a^a_{bc} = da^a_{bc} + a^d_{bc}\omega^a_d - a^a_{dc}\omega^d_b - a^a_{bd}\omega^d_c = 0;$$

$$\nabla a^a_{bu} = da^a_{bu} + a^d_{bu}\omega^a_d - a^a_{du}\omega^d_b - a^a_{bd}\omega^d_u = -(a^c_{uv}a^a_{cb} + a^c_{vb}a^a_{cu} + a^c_{bu}a^a_{cv})(\underset{1}{\omega}{}^v - \underset{2}{\omega}{}^v);$$

$$\nabla a^a_{uv} = da^a_{uv} + a^d_{uv}\omega^a_d - a^a_{dv}\omega^d_u - a^a_{ud}\omega^d_v = -b^a_{[uv]w}(\underset{1}{\omega}{}^w - \underset{2}{\omega}{}^w);$$

$$\nabla a^a_{uv} = da^a_{uv} + a^d_{uv}\omega^a_d - a^a_{dv}\omega^d_u - a^a_{ud}\omega^d_v = (\frac{1}{2}b^a_{wuv} - (a^b_{uv}a^a_{bw} + a^b_{vw}a^a_{bu} + a^b_{wu}a^a_{bv}))(\underset{1}{\omega}{}^w - \underset{2}{\omega}{}^w);$$

$$\nabla b^a_{cuv} = db^a_{cuv} + b^b_{cuv}\omega^a_b - b^a_{buv}\omega^b_c = 0;$$

$$\nabla b^a_{wuv} = db^a_{wuv} + b^b_{wuv}\omega^a_b - b^a_{buv}\omega^b_w = 0.$$

Эта система замкнута относительно внешнего дифференцирования.

7. В построенном адаптированном репере тензор кручения ткани B^{∇}_m удовлетворяет, помимо обобщенного тождества Якоби, еще некоторым соотношениям третьей и четвертой степени.

8. Три-ткань B^{∇}_m ранга ρ допускает нормальную подткань $\widetilde{W}$, которая является групповой, причем соответствующая фактор-ткань $W_1 = W/\widetilde{W}$ является регулярной.

В настоящей работе подробно исследуются ткани CB^{∇}_m, для которых $a^a_{bc} = 0$. В этом случае

9. Операторы $A_u = (a^a_{bu})$ порождают линейную алгебру Ли $[\bar{\mathscr{A}}]$. Эта алгебра является нильпотентной высоты 2.

Полностью описаны ткани, у которых алгебра $[\bar{\mathscr{A}}]$ является тривиальной, то есть все операторы A_u попарно коммутируют. Эти ткани обозначаем $CB^{\nabla}_m(1)$ — общий случай, и $CB^{\nabla}_m(0)$ — все операторы A_u имеют простую структуру.

10. Для тканей $CB^{\nabla}_m(0)$ существует семейство адаптированных реперов, в которых все операторы A_u становятся скалярными. Три-ткань $CB^{\nabla}_m(0)$ обладает замкнутой G_W-структурой класса 2 и является G-тканью, то есть допускает транзитивную группу автоморфизмов. При некотором выборе параметров слоений уравнения три-ткани $CB^{\nabla}_m(0)$ приводятся к виду

$$Z^a = X^a + e^{2a^a_{au}X^u}\left(Y^a - \frac{1}{4}\lambda^a_{vz}(X^vY^z - X^zY^v)\right), \quad Z^u = X^u + Y^u.$$

Найдена и проинтегрирована система структурных уравнений тканей $CB^{\nabla}_m(1)$.

12. В некоторых локальных координатах уравнения ткани $CB_m^{\nabla}(1)$ имеют вид:

$$Z^a = X^a + e_b^a(X)\left(Y^b - \frac{1}{2}d_{uv}^b(X^uY^v - X^vY^u) - \Lambda_{(uw)v}^b X^uX^wY^v\right) + \\ + \frac{2}{3}S_c^a(X)a_{b(t}^c\Lambda_{uw)v}^b X^tX^uX^wY^v,$$
$$Z^u = X^u + Y^u.$$

Этот класс тканей зависит от параметров a_{bu}^a — компонент тензора кручения, входящих в функции $e_b^a(X)$ и $S_c^a(X)$, постоянных d_{uv}^b и Λ_{uvw}^b. Функции $S_c^a(X)$ находятся из дифференциальных уравнеинй

$$S'(x)C(x) + 3S(x) = 3\exp(2C(x)),$$

где штрих обозначает формальную производную по C, $C(x) = (a_{bu}^a x^u)$, и удовлетворяют уравнению

$$S(x)C^3(x) = \frac{3}{2}\exp(2C(x))\left(C(x) - \frac{1}{2}E\right)^2.$$

Литература

1. Chern, S.S. *Eine Invariantentheorie der Dreigewebe aus r-dimensionalen Mannigfaltigkeiten in $\mathbf{R}_{2r}$* // Abh. Math. Sem. Univ. Hamburg. – 1936. – B. 11, no. 1–2. – S. 333–358.

2. Акивис М.А., Шелехов А.М. *Geometry and Algebra of Multidimensional Three-Webs.* – Dordrecht/Boston/London: Kluwer Academic Publishers, 1992. – xvii+358 p.

3. Bol G. *Gewebe und Gruppen* // Math. Ann. – 1937. – B. 114. – S. 414–431.

BOL THREE-WEBS WITH COVARIANT CONSTANT CURVATURE TENSOR

E.A. Onoprienko, A.M. Shelekhov

Infinitesimal properties of multidimensional middle Bol three-webs with covariantly constant curvature tensor (B_m^{∇} webs) are considered; we laid the foundations of the classification of such webs according to the rank of the torsion tensor. For a three-web B_m^{∇} of rank ρ, an adapted frame is constructed using the E. Cartan method, and a corresponding system of structure (differential) equations is found. It is proved that the three-web B_m^{∇} of rank ρ bears a normal subweb which is a group-web, and the corresponding factor-web is a regular three-web. By integration of the structure equations, new families of examples of multidimensional three-webs of a special type and smooth Bol loops are found; they are generalizations of the semidirect product of two abelian Lie groups.

Keywords: multidimensional three-web, Bol three-web, group three-web, elastic three-web, G-web, smooth Bol loop.

УДК 517.95

ОБ ОДНОЙ КРАЕВОЙ ЗАДАЧЕ ДЛЯ УРАВНЕНИЯ ЧЕТВЁРТОГО ПОРЯДКА С НЕОДНОРОДНЫМИ КРАЕВЫМИ УСЛОВИЯМИ

Ж.А. Отарова[1]

1 *j.otarova@mail.ru*; Каракалпакский государственный университет

В данной работе для уравнения четвёртого порядка в прямоугольной области на основе спектрального метода доказаны теоремы единственности и существования решения краевой задачи.

Ключевые слова: краевая задача, ряд Фурье, полнота, неоднородные условия.

1. Постановка задачи А. В области $\Omega = \{(x,t) : 0 < x < p,\ 0 < t < T\}$ рассмотрим краевую задачу для уравнения

$$u_{xxxx} + u_{tt} = f(x,t), \tag{1}$$

Задача *A*. Найти в области Ω решение $u(x,t)$ уравнения (1), удовлетворяющее краевым условиям

$$u(x,0) = \psi_1(x), \qquad 0 \le x \le p, \tag{2}$$

$$u_t(x,0) = \psi_2(x), \qquad 0 \le x \le p, \tag{3}$$

$$u(0,t) = \varphi_1(t), \qquad 0 \le t \le T, \tag{4}$$

$$u(p,t) = \varphi_2(t), \qquad 0 \le t \le T, \tag{5}$$

$$u_{xx}(0,t) = \varphi_3(t), \qquad 0 \le t \le T, \tag{6}$$

$$u_{xx}(p,t) = \varphi_4(t), \qquad 0 \le t \le T. \tag{7}$$

Краевые задачи для уравнения (1) с однородными краевыми условиями изучены в работах [1], [3]-[5].

Определение. Пусть $f(x,t) \in C(\Omega)$. Функцию $u(x,t) \in C^{2,1}_{x,t}\left(\overline{\Omega}\right) \cap C^{4,2}_{x,t}(\Omega)$ назовем регулярным решением задачи A, если она в области Ω удовлетворяет условиям (2)-(7) и уравнению (1).

2. Единственность решения задачи А.

Теорема 1. *Если существует регулярное решение $u(x,t)$ задачи А, то оно единственно.*

Доказательство. Пусть существуют два решения $u_1(x,t)$ и $u_2(x,t)$ задачи. Их разность удовлетворяет соответствующему однородному уравнению (1) и соответственно однородным условиям (2)-(7). Обозначим эту разность через $u(x,t)$, т. е.

$$u(x,t) = u_1(x,t) - u_2(x,t). \tag{8}$$

Известно, что функции

$$X_n(x) = \sqrt{\frac{2}{p}} \sin \lambda_n x, \ \ \lambda_n = \frac{n\pi}{p}, \ \ n = 1,2,\ldots \tag{9}$$

образуют в $L_2(0,p)$ полную ортонормированную систему.

Следуя [2], рассмотрим функции

$$d_n(t) = \int_0^p u(x,t)\, X_n(x)\, dx, \;\; n = 0,1,\ldots . \tag{10}$$

На основании (10) введём функции

$$d_{n,\varepsilon}(t) = \int_{\varepsilon}^{p-\varepsilon} u(x,t) \cdot X_n(x)\, dx, \quad 0 < \varepsilon < p, \tag{11}$$

где ε – таково, что $(\varepsilon, p-\varepsilon) \neq \emptyset$. Дифференцируя равенство (11) по t дважды, из уравнения (1) получаем

$$d_{n,\varepsilon}{}''(t) = -\int_{\varepsilon}^{p-\varepsilon} u_{xxxx}(x,t) \cdot X_n(x)\, dx. \tag{12}$$

Интегрируя правую часть (12) четыре раза по частям, переходим к пределу при $\varepsilon \to 0$, С учётом соответствующих однородных условий (4)-(7), которые следуют из (8), получаем

$$d_n{}''(t) = -\lambda_n^4 \int_0^p u(x,t)\, X_n(x)\, dx, \;\; n = 0,1,\ldots$$

В последнем равенстве, учитывая (10), имеем $d_n''(t) + \lambda_n^4 d_n(t) = 0, \;\; n = 0,1,\ldots$, т. е. получаем обыкновенное дифференциальное уравнение. Решая его и учитывая условия (2) и (3), имеем

$$\int_0^p u(x,t)\, X_n(x)\, dx = 0, \;\; n = 0,1,.. \tag{13}$$

Из (13) следует ортогональность $u(x,t)$ полной системе функций (9).

Следовательно, $u(x,t) \equiv 0$. В силу (8), получаем, что $u_1(x,t) \equiv u_2(x,t)$, т. е. решение задачи единственно. Теорема доказана.

3. Существование решения задачи А.

Теорема 2. *Если* $f(x,t) \in C_{x,t}^{2,0}\left(\overline{\Omega}\right)$, $f_{xx} \in L_2(\Omega)$, $f(0,t) = f(p,t) = 0$, $\forall\, t \in [0;T]$, *и* $\psi_3^{(4)}(x) \in C[0,p]$, $\psi_3^{(5)} \in L_2(0,p)$ *и удовлетворяет условиям* $\psi_3{}'(0) = \psi_3{}'(p) = 0$, $\psi_3{}'''(0) = \psi_3{}'''(p) = 0$; *а* $\psi_4^{(2)}(x) \in C[0,p]$, $\psi_4^{(3)}(x) \in L_2(0,p)$, *и удовлетворяет условиям* $\psi_4{}'(0) = \psi_4{}'(p) = 0$, *то регулярное решение задачи А существует и* $u(x,t) \in C_{x,t}^{4,2}\left(\overline{\Omega}\right)$. *(Функции* $\psi_3(x)$, $\psi_4(x)$ *определим ниже.)*

Доказательство. Введём вспомогательную функцию

$$w(x,t) = \varphi_1(t) + [\varphi_2(t) - \varphi_1(t)] \cdot \frac{x}{p} + \frac{p^2}{8\pi^2}[\varphi_4(t) + \varphi_3(t)] \times$$
$$\times \left(1 - \cos\frac{2\pi}{p}x\right) + \frac{p^2}{2\pi^2}[\varphi_4(t) - \varphi_3(t)] \cdot \left(\cos\frac{\pi}{p}x - 1 + \frac{2x}{p}\right), \tag{14}$$

Тогда решение задачи в виде суммы

$$u(x,t) = v(x,t) + w(x,t), \tag{15}$$

где, $v(x,t)$ – новая неизвестная функция. Таким образом, согласно (15) мы приходим к следующей задаче:

Задача $\widetilde{A}$. Найти в области Ω решение $v(x,t)$ уравнения

$$v_{xxxx} + v_{tt} = g(x,t), \tag{16}$$

удовлетворяющее краевым условиям

$$v(0,t) = v\left(p,t\right) = 0, \quad , \quad 0 \le t \le T, \tag{17}$$

$$v_{xx}(0,t) = v_{xx}\left(p,t\right) = 0, \quad 0 \le t \le T, \tag{18}$$

$$v(x,0) = \psi_3(x), \qquad 0 \le x \le p, \tag{19}$$

$$v_t(x,0) = \psi_4(x), \qquad 0 \le x \le p, \tag{20}$$

где

$$\psi_3(x) \equiv \psi_1(x) - w(x,0), \quad 0 \le x \le p,$$

$$\psi_4(x) \equiv \psi_2(x) - w_t(x,0), \quad 0 \le x \le p,$$

согласно (15).

Решение уравнения (16) ищем в виде ряда

$$v(x,t) = \sum_{n=0}^{\infty} v_n(t) \cdot X_n(x), \tag{21}$$

где $X_n(x)$ определены в (9). Тогда получим уравнение

$$v_n{}''(t) + \lambda_n^4 v_n(t) = g_n(t), \quad n = 0,1,...,$$

определяющее функции $v_n(t)$. Его решение имеет вид:

$$v_n(t) = a_n(0)\cos\lambda_n^2 t + b_n(0)\sin\lambda_n^2 t + \frac{1}{\lambda_n^2}\int_0^t g_n(\tau)\cdot\sin\lambda_n^2(t-\tau)\,d\tau, \quad n = 1,2,...$$

$$v(x,t) = \sqrt{\frac{2}{p}}\sum_{n=1}^{\infty}\left[a_n(0)\cos\lambda_n^2 t b_n(0)\sin\lambda_n^2 t + \frac{1}{\lambda_n^2}\int_0^t g_n(\tau)\cdot\sin\lambda_n^2(t-\tau)\,d\tau\right]\cdot sin\lambda_n x. \tag{22}$$

Неизвестные коэффициенты $a_n(0)$, $b_n(0)$ находим, используя (19), (20):

$$a_n(0) = \sqrt{\frac{2}{p}}\int_0^p \psi_3(x)\sin\lambda_n x dx, \quad n = 1,2,...$$

$$b_n(0) = \sqrt{\frac{2}{p}}\frac{1}{\lambda_n^2}\int_0^p \psi_4(x)\sin\lambda_n x dx, \quad n = 1,2,...$$

Таким образом, решение задачи представляется в виде (22), где $a_n(0)$, $b_n(0)$ определяются формулами, приведенными выше. Следовательно, мы построили формальное решение задачи $\widetilde{A}$ в области Ω, которое даётся формулой (21).

Лемма 1. $\forall\, t \in [0;T]$ при $n = 1,2,..$ справедливы оценки

$$|v_n(t)| \le [|a_n(0)| + |b_n(0)|] + \frac{\sqrt{T}}{\lambda_n^2}\|g_n\|_{L_2(0;T)},$$

$$|v_n'(t)| \le \lambda_n^2 [|a_n(0)| + |b_n(0)|] + \sqrt{T}\|g_n\|_{L_2(0;T)},$$

$$|v_n''(t)| \le \lambda_n^4 [|a_n(0)| + |b_n(0)|] + C\|g\|_{C\left(\overline{\Omega}\right)} + \lambda_n^2\sqrt{T}\|g_n\|_{L_2(0;T)},$$

где $C = \text{const} > 0$.

Замечание. Из леммы следует, что $u(x,t) \in C_{x,t}^{4,2}\left(\overline{\Omega}\right)$.

Литература

1. Аманов Д. *Вольтерровость краевой задачи для уравнения четвертого порядка* // Спектр. теория дифф. операторов и родств. пр.: Тр. межд. конф. 24-28 июня 2003. – Т. 1. – Стерлитамак, 2003. – С. 78–82.

2. Моисеев Е.И. *О решении спектральным методом одной нелокальной краевой задачи* // Дифф. ур. – Киев, 1999. – № 8 (35). – С. 1094–1100.

3. Отарова Ж.А. *Разрешимость и спектральные свойства самосопряженной задачи для уравнения четвертого порядка* // Докл. АН РУЗ. – Ташкент, 2008. – № 1. – С. 10–14.

4. Отарова Ж.А. *Разрешимость и спектральные свойства самосопряженных задач для уравнения четвертого порядка* // Узб. мат. журн. – Ташкент, 2008. – № 2. – С. 74–80.

5. Otarova J.A. *Volterraness of boundary value problem for fourth order equation* // The Journal of Arts and Science (Sakarya University Faculty of Arts and Science), 2007. – № 9. – P. 152–162.

BOUNDARY VALUE PROBLEM FOR DIFFERENTIAL FOURTH ORDER EQUATION WITH INHOMOGENEOUS BOUNDARY CONDITIONS

J.A. Otarova

In the given work, for a fourth order differential equation in a rectangular domain, on the basis of the spectral method, theorems of uniqueness and existence of solution are established.

Keywords: boundary value problem, number Fourier, completeness, nonuniform conditions.

УДК 512.554

ТРЕХМЕРНЫЕ КВАЗИПОЛЯ С ДВУСТОРОННЕЙ ДИСТРИБУТИВНОСТЬЮ

С.В. Панов[1]

1 *pansevakrasn@mail.ru*; Сибирский федеральный университет, Институт математики и фундаментальной информатики

В статье рассматривается строение полуполей, представляющих собой трехмерные линейные пространства над своими ядрами.

Ключевые слова: квазиполе, полуполе.

В соответствии с [1], *квазигруппой* называют систему элементов $W(a,b,c,...)$ с такой бинарной операцией умножения $\circ$, что в равенстве $a \circ b = c$ любые два из элементов a, b, c системы W однозначно определяют третий. Квазигруппа с единицей e является *лупой*.

Если Q – непустое множество с двумя бинарными операциями $+$ и $\circ$, при этом $(Q,+)$ – абелева группа, а $(Q^*,\circ)$ – лупа, где $Q^* = Q \setminus \{0\}$, и выполняется односторонняя дистрибутивность, то $(Q,+,\circ)$ называют *квазиполем*.

Полуполе – это квазиполе с двусторонней дистрибутивностью. *Собственным полуполем* называют всякое полуполе, не являющееся полем [2].

Левым, *правым* и *средним ядрами* полуполя $(S,+,\circ)$ называют соответственно множества:

$$N_l = \{l \in S | \forall a,b \in S : (l \circ a) \circ b = l \circ (a \circ b)\};$$

$$N_m = \{m \in S | \forall a,b \in S : (a \circ m) \circ b = a \circ (m \circ b)\};$$

$$N_r = \{r \in S | \forall a,b \in S : (a \circ b) \circ r = a \circ (b \circ r)\}.$$

Ядром полуполя S называют множество $N(S) = N_l \cap N_m \cap N_r$, а *центром* – такое множество $Z(S)$, что каждый его элемент коммутирует с любым $s \in S$. Известно, что полуполе можно рассматривать как левое (правое) векторное пространство над своими левым ядром N_l (правым ядром N_r) или как двустороннее векторное пространство над $N(S)$ или $Z(S)$ [2].

Работы, посвященные изучению конечных квазиполей, возникли в начале прошлого века и были тесно связаны с вопросами построения проективных плоскостей трансляций. Они восходят к таким авторам, как L. Dickson ([3] и др.), O. Veblen, J. H. Maclagan-Wedderburn [4]. В отличии от конечных полей, теория которых изучена хорошо, для квазиполей и полуполей даже малых порядков p^n (p – простое число) до сих пор остаются открытыми вопросы строения [2], [5]. В этой работе рассматриваются исключительно полуполя, являющиеся трехмерными пространствами над своими ядрами или центром.

Теорема 1. *Если в полуполе S порядка p^3 всякий элемент s лежит в каком-либо подполе порядка $\le p^2$, то S – поле.*

Из теоремы 1 следует, что подполе $GF(p)$ – максимальное подполе полуполя S порядка p^3, а в качестве базы S можно выбрать $\{e, x, x^2\}$ для некоторого $x \in S$, не

лежащего в единственном подполе. Опираясь на это, мы получили следующий результат:

Теорема 2. *Всякое собственное полуполе S порядка p^3 (p – простое число) содержит элемент x, удовлетворяющий либо условию $xx^2 \neq x^2x$, либо с условиям $xx^2 = x^2x$ и $xx^3 \neq x^2x^2$.*

Если лупа $(S^*, \circ)$ полуполя S коммутативна, то обе перечисленные теоремы легко обобщаются на случай произвольного трехмерного полуполя порядка q^3, рассмотренного над своим ядром порядка $q = p^n$ (n – натуральное число).

Работа выполнена при финансовой поддержке РФФИ (проект 16-31-00173).

Литература

1. Холл М. *Теория групп.* – М.: ИЛ, 1962. – 468 с.

2. Johnson N. L., Jha V., Biliotti M. *Handbook of finite translation planes.* – London: Taylor & Francis, 2007. – 861 p.

3. Dickson L. E. *Linear algebras in which division is always uniquely possible* // Trans. Amer. Math. Soc. – 1906. – № 7. – P. 370–390.

4. Veblen O., Maclagan-Wedderburn J. H. *Non-Desarguesian and non-Pascalian geometries* // Trans. Amer. Math. Soc. – 1907. – V. 8. – No. 3. – P. 379–388.

5. Levchuk V. M., Panov S. V., Shtukkert P. K. *The structure of finite quasifields and their projective planes* // Proc. XII Intern. Conf. on Algebra and Number Theory. – Tula, 2014. – P. 106–108.

THREE-DIMENSIONAL QUASIFIELDS SATISFYING BOTH DISTRIBUTIVE LAWS

S.V. Panov

The article deals with the structure of semifields which are linear spaces over their nuclei.

Keywords: quasifield, semifield.

УДК 519.7

О НЕКОТОРЫХ СХЕМАХ ЧАСТИЧНЫХ ЗАТЕМНЕННЫХ ПОДПИСЕЙ, ПОДОБНЫХ ПОДПИСИ RSA

О.Ю. Петров[1]

1 *olezhpetrov@gmail.com*; Казанский (Приволжский) федеральный университет, Институт математики и механики

В статье приведены новые примеры частичных затемненных подписей.

Ключевые слова: цифровая затемненная подпись, частичная затемненная подпись, RSA.

Введение в затемненные цифровые подписи (blind signatures) можно найти в [1]. В этой статье они называются подписями “вслепую”. Важной разновидностью затемненных подписей являются частичные затемненные подписи (partially blind

signatures), впервые определенные в статье [2]. В этой работе конструируется частично затемненная подпись на основе известной цифровой подписи RSA. В нашей работе предлагается еще несколько вариантов подобных подписей.

Неформально идею частичной затемненной подписи можно объяснить на примере использования обычной затемненной подписи для создания электронных денег (e-cash) [3]. В описанном в [3] протоколе действует Покупатель, который желает получить из Банка электронную наличность для дистанционной покупки, и Банк, который подписывает "вслепую" присланный Покупателем затемненный идентификатор банкноты. При этом возникает проблема: как Покупателю снять со счета ту сумму, которую он пожелает, а не какую-то жестко зафиксированную. Одним из решений этой проблемы является введение в подпись открытого параметра, имеющего смысл той суммы, которую надо снять со счета.

Будем использовать обозначения и соглашения из [3, с. 65–67]. В частности, $N = pq$ — модуль RSA, e — шифрующая экспонента, $ed = 1 + \varphi(N)u$, f — открытая односторонняя функция. Через m обозначается идентификатор банкноты, который случайным образом генерирует Покупатель, через t — открытый параметр, имеющий смысл снимаемой со счета суммы. Значение d знает только Банк.

1) Покупатель формирует число $(f(m)r^e)^t \pmod N$ и отправляет банку вместе с t. Число r (затемнение) взаимно просто с N.

2) Банк подписывает: $(f(m)^t r^{et})^d \pmod N = f(m)^{td}(r^{ed})^t = f(m)^{td} r^t \pmod N$. Полученное выражение отправляет покупателю.

3) Покупатель может снять затемнение, так как на r^t можно делить.Таким образом, $s = f(m)^{td} \pmod N$

Электронной банкнотой номиналом в t единиц будет являться тройка $(m, (f(m))^{td}, t)$.

Проверка подписи: если получена банкнота вида (m, s, t), то надо проверить сравнение:

$$f(m)^{td} \equiv s^{td} \pmod N.$$

Предложим еще один вариант использования открытого параметра t.

1) Покупатель формирует число $(f(m)r^e t)^d$, и отправляет банку вместе с t.

2) Банк подписывает: $(f(m)r^e t)^d \pmod N = f(m)^d (r^{ed}) t^d = f(m)^d t^d r \pmod N$. Полученное выражение отправляет покупателю.

3) Покупатель может снять затемнение, так как на r можно делить.Таким образом, $s = f(m)^d t^d \pmod N$

Электронной банкнотой номиналом в t единиц будет являться тройка $(m, (f(m))^d t^d, t)$.

Проверка подписи: если получена банкнота вида (m, s, t), то надо проверить сравнение:

$$f(m)^d t^d \equiv s^d t^d \pmod N.$$

Общее требование к таким протоколам: невозможности изменить параметр t после того, как проведено подписание.

Рассмотрим еще одну частичную затемненную подпись, которая строится на основе одной подписи из [4]. Здесь p, q — большие простые числа, $q|p-1$, $Z_p = \{0, 1, \ldots, p-1\}$, и аналогично Z_q. Элемент $\alpha \in Z_p$ имеет порядок q. s_N — секретный ключ Банка, $p_N = \alpha^{s_N}$ — открытый ключ.

1) Банк выбирает случайное число $\tilde{k} \in Z_q$ и вычисляет $\tilde{r} \equiv \alpha^{\tilde{k}} \pmod{p}$
2) Отправляет $\tilde{r}$ покупателю.
3) Покупатель выбирает случайные числа $a, b \in Z_q$ и вычисляет $r := \tilde{r}^{-a}\alpha^b \pmod{p}$ и $\tilde{m} = a^{-1}(m+r) - \tilde{r} \pmod{q}$.
4) Вместе с $\tilde{m}$ покупатель отправляет банку параметр t.
5) Банк подписывает затемненное сообщение $\tilde{m}$, вычисляя $\tilde{s} \equiv (\tilde{m} + \tilde{r}) s_N t - \tilde{k}$.
6) Отправляет $\tilde{s}$ покупателю, который вычисляет $s = a\tilde{s} + b - r \pmod{q}$.

$(m; r, s, t)$ — подписанное сообщение.

Проверка подписи:

$$\alpha^s \equiv p_N^{(m+r)t} r \alpha^{-r} \pmod{p}.$$

Литература

1. Епишкина А. В., Шимкив М. Я. *Обзор и анализ криптографических схем, реализующих электронную подпись «вслепую»* // Безоп. инф. техн. – 2015. – № 3. – С. 51–58.

2. Abe M., Fujisaki E. *How to date blind signatures* // Advances in Cryptology – AisaCrypt'96, Springer-Verlag, 1996, LNCS 1163. – P. 244–251.

3. *Введение в криптографию*/ Под общ. ред. В. В. Ященко. – 4-е изд., доп. – М.: МЦНМО, 2012. – 348 с.

4. Horster P. Michels M., Petersen H. *Efficient blind signature schemes based on the discrete logarithm problem* // Univ. of Technol. Chemiitz-Zwickau, Techn. Report TR-94-6-D. – 1994. – 5 p.

ABOUT SOME SCHEMES OF RSA-BASED PARTIAL BLIND SIGNATURES

O.Y. Petrov

The article gives new examples of partial blind signatures.

Keywords: digital blind signature, partial blind signature, RSA.

УДК 519.688, 511.174

НЕКОТОРЫЕ ВОПРОСЫ АДДИТИВНОЙ ТЕОРИИ ЧИСЕЛ

Н.В. Потапова[1], А.В. Рожков[2]

1 *potapova50@gmail.com*; Кубанский государственный университет
2 *ros.seminar@bk.ru*; Кубанский государственный университет

В различных системах счисления изучается функция нахождения суммы цифр чисел в композиции с арифметическими функциями.

Ключевые слова: теория чисел, факториал, пакеты компьютерной алгебры, криптография, хэш-функции, однонаправленные функции.

Введение

Первоначальная цель работы была в основном методическая: продемонстрировать на простых арифметических примерах важнейшие и плохо разработанные понятия современной криптографии, такие как хэш-функции и однонаправленные функции, существование которых, кстати, до сих пор строго не доказано [3].

Определение. *Функция χ, ставящая в соответствие сообщению произвольной длины сообщение фиксированной длины, называется хэш-функцией. Эквивалентно, отображение $\chi : \mathbb{N} \to \mathbb{N}$, имеющее конечный образ называется хэш-функцией.*

Определение. *Функция $\psi : \mathbb{N} \to \mathbb{N}$ называется однонаправленной, если для любого $n \in \mathbb{N}$ образ $\psi(n) = m$ вычисляется за полиномиальное время, но не существует полиномиального алгоритма, вычисляющего прообраз n образа m.*

Введем основное определение нашей работы. Пусть задана некоторая система счисления, например, десятичная.

Определение. *Пусть $a \in \mathbb{N}$, и $a = \overline{a_1 a_2 \ldots a_n}$ — (десятичная) запись числа a. Функцией суммы назовем отображение $S(a) = a_1 + a_2 + \ldots + a_n$.*

Функция суммы во многих отношениях хорошо моделирует и поведение хэш функции и однонаправленной функции.

В самом деле, современные хэш-функции имеют, в основном, 512 битный образ, другими словами $|\chi(\mathbb{N})| \leq 2^{512}$.

Поскольку $S(a) < 9 * \lg(a)$, то ограничение $S(a) \leq 2^{512}$ означает, что

$$a \leq 10^{\frac{1}{9} \cdot 2^{512}} \approx 10^{(10^{150})}.$$

Это фантастически большое число. Так, размер видимой части вселенной равен примерно 10^{26} m., а ее объем, соответственно, 10^{78} m^3. Даже если заполнить нашу Вселенную частицами планковской длины 10^{-35}, имеющих объем 10^{-105}, то нам потребуется всего 10^{183} частиц — ничтожнейшее число, по сравнению с монстром $10^{(10^{150})}$. Поэтому с практической точки зрения функция суммы цифр – очень хороший кандидат на роль хэш-функции.

Однако поведение функции $S(a)$ весьма прихотливо. Загадочна связь суммы цифр произведения с суммой цифр сомножителей. В самом деле,

$$S(2^{10}) = S(1024) = 7, S(5^{10}) = S(8765625) = 40, S(2^{10} \cdot 5^{10}) = 1.$$

Не лучше обстоит дело и при работе с суммой чисел. Например, $S(44445) = 21$, $S(55555) = 25$, но $444445 + 55555 = 1000000$.

Сумма цифр факториала натурального числа

Были использованы идея и методология, предложенная в работах [1], [2]. Вычисления производились с использованием пакета компьютерной алгебры gap4.8.8. официальный адрес http://www.gap-system.org/

На нахождение суммы цифр факториала нас вдохновила формула Стирлинга:

$$n! \approx \sqrt{2n\pi}\left(\frac{n}{e}\right)^n.$$

Обширный численный эксперимент, занявший около 300 часов и проводившийся на процессоре Core i5 4430 3 Ггц, позволил нам выдвинуть гипотезу, что $|F(n)| < 1$ для любого $n > 100$, где

$$F(n) = \frac{S(n!)}{n} - 2\ln\frac{n}{2} + 2.$$

Вычисления проводились до $n = 10^6$. Миллион факториал содержит примерно 5 млн. десятичных знаков.

Утверждение. *Для* $100 < n < 10^6$ *были получены следующие результаты:*

1. Для всех n выполняется неравенство $|F(n)| < 1$.

2. Математическое ожидание функции $F(n)$ *быстро стремится к 0: при* $n > 10^4$ *оно не превышает по модулю* 10^{-5}*, а при* $n > 10^5$ *модуль матожидания не превышает* 10^{-6}.

3. Дисперсия функции $F(n)$ *при* $n > 10^5$ *не превышает* $0,001$.

4. Плотность распределения значений функции $F(n)$*, если считать ее случайной величиной, близка к нормальной.*

Теперь остается дать теоретическое обоснование этого результата.

Некоторые обобщения

Сумма цифр числа зависит от системы счисления. Нами были проведены вычисления для k-значных систем, $k \in \{2, 10, 17, 197\}$.

По результатам вычислений была выдвинута гипотеза, что для любой k-значной системы существуют такие действительные положительные числа A, B, C и такое натуральное число N, что для всех $n > N$ выполняется неравенство

$$\left|\frac{S(n!)}{n} - A\ln(n) + B\right| < C.$$

Для перечисленных выше значений k вычисления позволили выдвинуть гипотезу, что

$$A = \frac{k}{2\ln(k)}, B = \sqrt{k}, C = \ln(k), N = 4 * 10^4.$$

Кроме суммы цифр факториала натурального числа мы также исследовали функции вида $f(n) = k^n$. Эти функции, в суперпозиции с функцией суммы цифр,

хорошо иллюстрируют и понятие хэш-функции и понятие однонаправленной функции. Дело в том, что для нахождения прообраза придет проверять экспоненциально много кандидатов.

Утверждение. *В десятичной системе счисления для всех натуральных* $k < 10$ *для функции* $S(k^n)$ *выполняется следующее неравенство*

$$n(1-\lg(k)) < S(k^n) < n(1+\lg(k)).$$

Аналогичные формулы имеют место и для других систем счисления.

Выводы

Предложены и в разумных пределах проверены интересные гипотезы о поведении функции суммы цифр натурального числа в разных системах счисления:

$$S(n!) \approx 2n\ln\frac{n}{2} - 2n,$$
$$n(1-\lg(k)) < S(k^n) < n(1+\lg(k)).$$

Эти результаты, возможно, могут быть обоснованы и теоретически. Кроме того, в учебно иллюстративных целях обе функции могут использоваться как хэш-функции, а вторая и как кандидат в однонаправленные функции.

Литература

1. Рожков А.В. *Стратегия DPS - Debian-Python-Sage: Проблемно-ориентированные вычислительные среды на открытом коде* // Труды V-я Междунар. Науч.-практич. Конф. «Информационные технологии в образовании и науке» (ИТОН – 2016) Казань: КФУ, 2016. – С. 172-179.

2. Рожков А.В., Рожкова М.В.*Экспериментальная (вычислительная) теория чисел* // Новые информационные технологии в образовании и науке: материалы X междунар. науч.-практ. конф., Екатеринбург, 27 февраля – 3 марта 2017 г. ФГАОУ ВО «Рос. гос. проф.-пед. ун-т». – Екатеринбург, 2017. – С. 413-417.

3. Рожков А.В., Ниссельбаум О.В. *Теоретико-числовые методы в криптографии*. – Тюмень: ТюмГУ, 2007. – 160 с.

SOME QUESTIONS OF THE ADDITIVE NUMBER THEORY

N.V. Potapova, A.V. Rozhkov

In different numeration systems, the function of finding of the sum of digits of numbers in composition with arithmetic functions is studied.

Keywords: the number theory, factorial, packages of computer algebra, cryptography, function hash, unidirectional functions.

УДК 004

РАЗРАБОТКА ANDROID-ПРИЛОЖЕНИЯ «ИНФОРМЕР ОСО КУБГУ»

Н.В. Потапова[1], Р.Ю. Селимов[2]

1 *potapova50@gmail.com*; Кубанский государственный университет
2 *selimov@gmail.com*; Кубанский государственный университет

Описана реализация студенческой информационной системы «Информер ОСО КубГУ» на базе ОС Android, ориентированной, в частности, на студентов Кубанского государственного университета.

Ключевые слова: Андроид-приложение, защита информации, Объединенный совет обучающихся, Кубанский государственный университет.

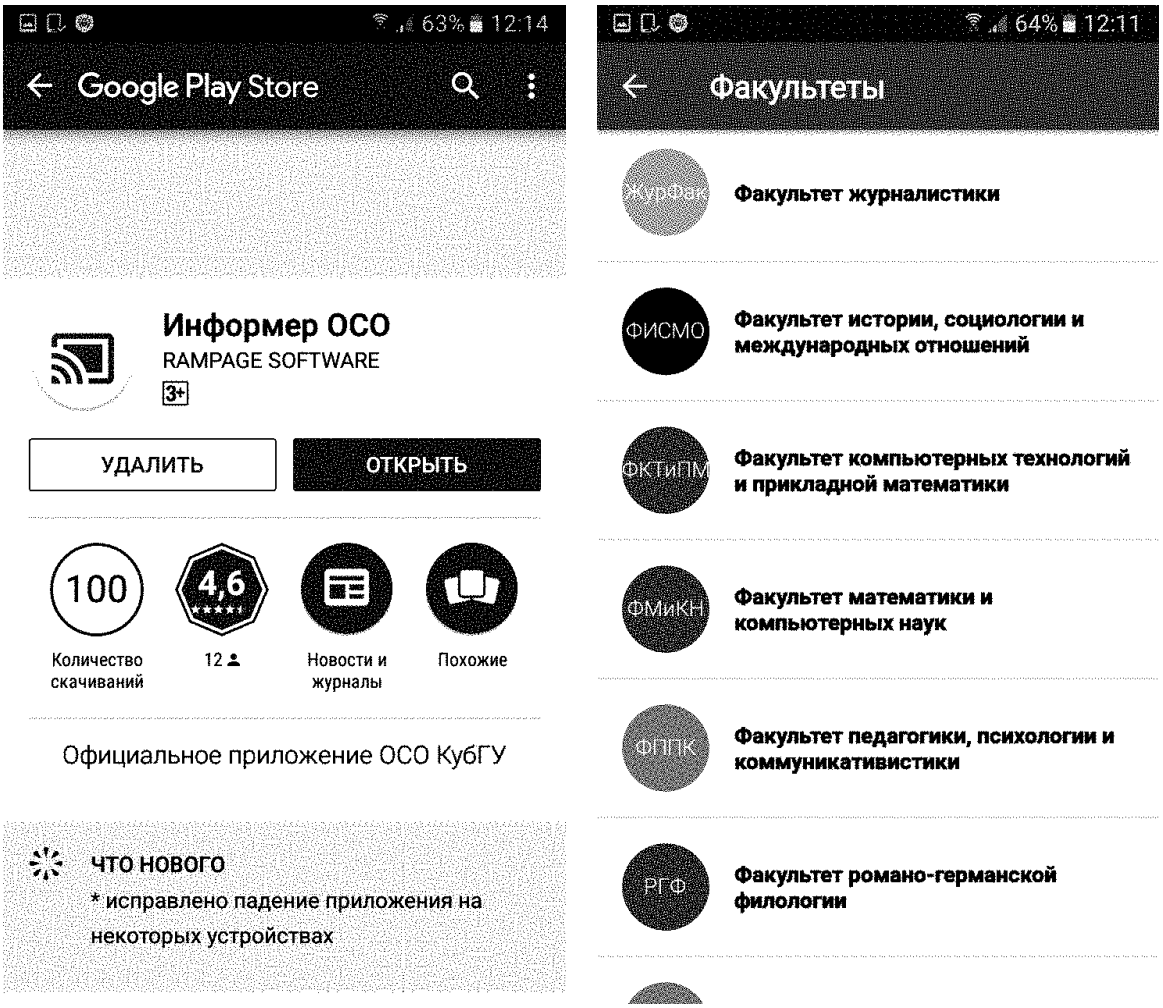
Стратегия развития информационного общества в Российской Федерации на 2017 — 2030 годы ставит конкретные цели и стратегические национальные приоритеты Российской Федерации при развитии информационного общества. Необходимо формирование информационного пространства с учетом потребностей граждан в получении качественных и достоверных сведений, развитие информационной и коммуникационной инфраструктуры, а также создание и применение российских информационных и коммуникационных технологий, обеспечение их конкурентоспособности на международном уровне.

Объединенный совет обучающихся Кубанского государственного университета (далее – ОСО КубГУ) был создан в 2013 году. За время работы ОСО КубГУ в его состав вошли студенческие советы 17 факультетов и были созданы 12 студенческих организаций. Общая численность актива составляет более 5000 человек. Это обусловливает необходимость иметь Кубанскому государственному университету и Объединенному совету обучающихся, в частности, свое информпространство.

Мобильные телефоны давно перестали быть роскошью и есть у каждого современного человека. Они отлично справляются со своей функцией – поддерживают коммуникацию между людьми. При этом, недавно появившиеся, но уже прочно обосновавшиеся в нашей жизни смартфоны настолько функциональны, что трудно сказать, чего они не умеют. По сути, смартфон стал небольшой копией компьютера, который постоянно можно иметь при себе и обмениваться с его помощью информацией из любой точки мира. В наше время все больше и больше смартфонов, коммуникаторов, планшетных ПК и других видов устройств, удобных для использования как в повседневной жизни, так и в образовательном или рабочем процессе, выпускаются на базе ОС Android. Основываясь на этом, было принято решение создать приложение «Информер ОСО КубГУ», которое позволило перевести всю деятельность нашей организации в электронный вид.

Приложение «Информер ОСО КубГУ» позволяет студентам:

- просматривать актуальные новости студенческих советов;
- следить за афишей мероприятий;
- быть в числе первых, кто узнает актуальную информацию о ВУЗе;
- получать сведения о каждом факультете и его деятельности;



(a). Установка на Play Store **(b).** Просмотр новостной ленты

Рис. 1. Пример работы с Информером

- получать push–уведомления;
- общаться с председателями организаций и факультетов.

Приложение «Информер ОСО КубГУ» доступно для скачивания любому пользователю, будь то студент, преподаватель или научный сотрудник Кубанского государственного университета. Наша информплощадка — отличный показатель развития информационного общества в образовательной сфере РФ и в КубГУ, в частности.

Удаленный сервер приложения работает на основе Ubuntu Server 16.04, в качестве веб-сервера выбран Nginx, а сервером базы данных является MariaDB, ответвление от СУБД MySQL. Скрипты, запускаемые на сервере, написаны на PHP7, результат их работы — данные в формате JSON — отправляются клиентской части приложения, где подвергаются парсингу и, впоследствии, отображаются в удобном для пользователя виде.

Клиентская часть разработана при помощи среды разработки (IDE) Android Studio (версия 2.3) с использованием языка программирования Java.

Элементы интерфейса построены при помощи xml — разметки. Помимо java —

и xml — файлов, в проект включены сборочные скрипты системы сборки Gradle.

Программные модули подразделяются на внешние (сторонние проекты) и внутренние. Причем последние, в свою очередь, подразделяются на следующие группы: global, push, activity, adapter, ui, util, stuff, parser, config, cache, network, fragment, service, radio и другие.

Global — глобальные переменные и константы, push — обеспечение получения мгновенных уведомлений, network — работа с сетью, service — фоновые службы приложения, radio — потоковое радио, config — работа с конфигурацией, cache — реализация кэша материалов, stuff и util — вспомогательные средства, ui — нестандартные элементы интерфейса, parser — парсер json, activity — код управления экранами интерфейса, adapter — реализации прокрутки списков, fragment — управление блоками элементов интерфейса.

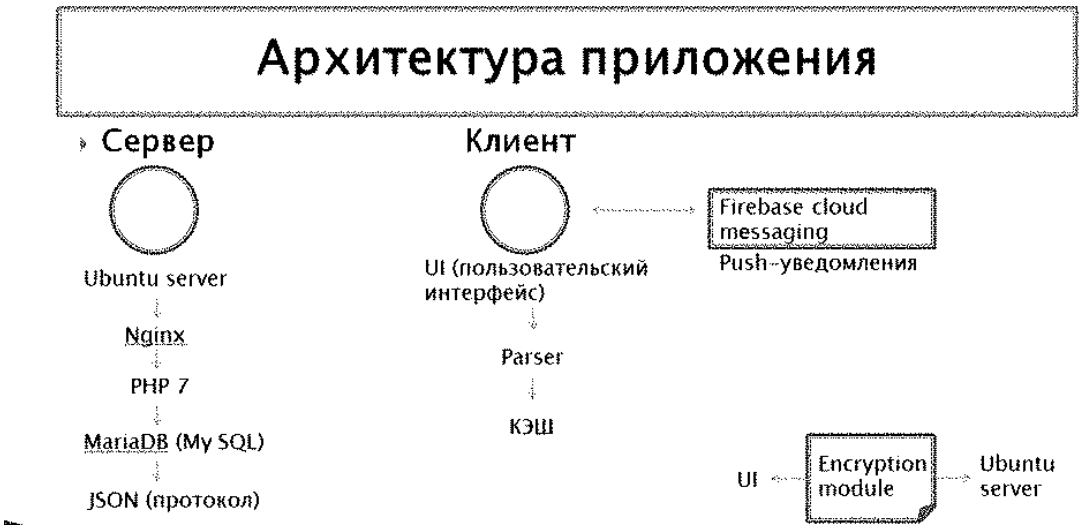


Рис. 2. Пример работы с Информером

Рассмотрим принцип работы. Пользователь вызывает срабатывание начала загрузки материала, например, смахиванием вниз ленты, тем самым начинается обновление новости, мероприятия и т.п. Это влечет за собой отправку запроса на сервер с параметрами количества запрашиваемых данных, информации об ОС, ее версии, а также информацию о клиенте и прочие данные. Сервер в свою очередь начинает обработку запроса, и по окончании выполнения скрипта (get.php), возвращает ответ клиенту в виде json – строки. Клиент, получая ответ сервера, вызывает метод класса Parser, соответствующий началу парсинга json – строки, и, в конечном итоге, мы получаем экземпляры классов NewsItem (EventItem или другие) с необходимыми для дальнейшей работы приложения заполненными полями, после происходит вывод данных на экран пользователя.

Также, стоит отметить, что все изображения используемые в Информере защищены цифровым водяным знаком, созданным при помощи онлайн сервера Watermark.Algid.Net. Для того чтобы создать водяной знак с помощью онлайн сервиса Watermark.Algid.Net, необходимо выбрать в главном меню сайта пункт «Сервисы» и перейти на подпункт «Водяной знак — текст» или «Водяной знак — изображение». После создания знака, выбираем файл изображения, на которое он будет

нанесен. Поддерживаются изображения форматов JPEG, GIF и PNG.

Для обмена важной информацией, было принято решение создать в приложении «Информер ОСО КубГУ» модуль защищенного электронного документооборота.

При запуске модуля на экране смартфона отображается кнопка для выбора и отправки файла, при нажатии которой открывается окно выбора файла. Следует отметить, что выбор возможен только текстового файла. После закрытия окна производится: считывание файла в память устройства с последующим шифрованием по алгоритму RSA и отправкой зашифрованных данных на сервер, где производится расшифровка данных и сохранение в БД.

При доступе к панели управления (с использованием учетной записи, созданной администратором) отображается список доступных файлов защищенного документооборота, которые можно скачать на локальное устройство, с которого производится доступ. Для обеспечения дополнительной безопасности при авторизации пользователя в панели управления и предотвращения перехвата данных мы используем https–сервер с ssl–сертификатом.

Информационные технологии прогрессируют очень быстро, охватывая все более широкие области человеческой деятельности. Поднимая вопрос о недостаточно уровне информационного общества РФ, нельзя не сказать об актуальности разработки программного приложения «Информер ОСО КубГУ», соответствующего тематике данной проблемы и реализованного в соответствие с новейшими информационными технологиями. «Информер ОСО КубГУ» поможет студентам иметь свое информационное пространство для получения качественных и достоверных сведений о работе Кубанского государственного университета.

Литература

1. Указ Президента Российской Федерации "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы"от 09.05.2017 № 203

2. Phillips B., Hardy B. *Android Programming: The Big Nerd Ranch Big*. – Nerd Ranch Guides, 2013.

3. Потапова Н.В. *Дистанционное образование, как электронный документооборот* // Инф. техн. в обр. и науке: Материалы Междунар. науч.-практ. конф., 5-7 нояб. 2016 г., г. Казань. КФУ. – Казань, 2016. – С. 166–172.

4. Потапова Н.В., Большакова А.А. *Php, Ruby, Python - на чем остановить свой выбор студенту при изучении веб-разработки?* // Новые инф. техн. в обр. и науке: НИТО-2017: материалы X международной научно-практической конференции, Екатеринбург, 27 февраля - 3 марта 2017 г. – Екатеринбург: РГППУ, 2017. – С. 409–413.

5. Потапова Н.В. *Программные комплексы электронного документооборота* // VIII межд. научн. конф. «Математика. Образование. Культура», посв. 240-летию со дня рождения К.Ф. Гаусса. 26–28 апреля 2017 г. – Тольяттинский гос. ун-т, г. Тольятти.

DEVELOPMENT OF ANDROID APPLICATION “INFORM OSO KUBSU”

N.V. Potapova, R.Y. Selimov

The implementation of the student information system “Informer OSO KubSU” based on the Android OS, is described.

Keywords: Android application, information protection, United Board of Learners, Kuban State University.

УДК 517.53

РАЗЛОЖЕНИЕ В РЯД ФУНКЦИЙ, АНАЛИТИЧЕСКИХ В ОГРАНИЧЕННОЙ ЗАМКНУТОЙ ОБЛАСТИ

А.И. Рафиков[1]

1 *azat@rafikov.me*; Башкирский государственный университет

В работе рассматривается частный случай задачи разложения функций, аналитических в замыкании ограниченной выпуклой области $\mathbb{C}$, в ряд по специальной системе экспоненциальных многочленов с правильно распределённой последовательностью показателей.

Ключевые слова: интерполяция, экспоненциальные многочлены, выпуклая область.

Пусть даны кратная последовательность комплексных чисел $\Lambda = \{\lambda_k, \nu_k\}$ с единственной предельной точкой ∞ и ограниченная выпуклая область $D \subset \mathbb{C}$. Обозначим символом $H(\overline{D})$ пространство функций, аналитических в замыкании области D, с топологией равномерной сходимости на компактах.

Наша задача — найти представление функций из этого пространства с помощью рядов экспоненциальных многочленов с показателями λ_n. Широко известен результат А. Ф. Леонтьева о разложении в ряд для случая, когда каноническое произведение $L(\lambda)$, построенное по точкам последовательности Λ, имеет хорошие оценки снизу, в частности, когда оно является функцией вполне регулярного роста [3, гл. IV, § 6, п. 4, теорема 4.6.8]:

$$f(z) = \lim_{k \to +\infty} \frac{1}{2\pi i} \oint\limits_{|\mu| = \rho_k} \frac{\omega_L(\mu, \alpha, f) e^{\mu z}}{L(\mu)} d\mu,$$

где $\omega_L(\mu, \alpha, f)$ — интерполирующая функция Леонтьева, $\alpha \in \mathbb{C}$ — параметр, а $0 < \rho_1 < \rho_2 < \rho_3 < \dots$ — неограниченная последовательность радиусов, для которой выполнены условия: $\rho_{k+1}/\rho_k \longrightarrow 1$ при $k \to +\infty$ и при любом $\varepsilon > 0$ найдётся номер $K(\varepsilon)$, начиная с которого на окружностях $\partial B(0, \rho_k)$ выполняется подходящая оценка снизу на $L(\lambda)$.

В данной работе показывается, что при применении техник, описанных в статьях [1] и [2], этот результат можно улучшить. Во-первых, существенно уменьшить разброс точек Λ внутри групп, перейдя от колец к «относительно малым» группам. Во-вторых, подобрать линейные комбинации элементов системы $\{z^k e^{\lambda_n z}\}_{n=1,k=0}^{+\infty,\nu_n-1}$ так, что разложения по ним имеют более простой вид. Наконец, записать условие теоремы в терминах геометрических характеристик последовательности.

Перед тем, как сформулировать результат, введём необходимые понятия и обозначения.

Семейство непустых множеств $U = \{U_m\}_{m=1}^{+\infty}$ назовём разбиением последовательности Λ, если все множества U_m состоят из точек Λ, попарно не пересекаются и $\bigcup\limits_{m=1}^{+\infty} U_m = \Lambda$. В таком случае естественно ввести ещё одну нумерацию точек Λ, зависящую от U. Точки группы U_m пронумеруем следующим образом: $\{\lambda_{m,k}\}_{k=1}^{N_m}$ (N_m —

количество точек λ_k, лежащих в U_m), кратность $\lambda_{m,k}$ обозначим через $\nu_{m,k}$. Разбиение U назовём относительно малым, если

$$\overline{\lim_{m\to+\infty}} \max_{1\le k,l\le N_m} \left|\frac{\lambda_{m,k}-\lambda_{m,l}}{\lambda_{m,k}}\right| = 0.$$

Наконец, через $W_D(\varphi,\psi)$ обозначим длину дуги этой области между точками касания опорных прямых, проведённых в направлениях $\arg t = \varphi$ и $\arg t = \psi$; за $W_\Lambda(\varphi,\psi)$ — функцию угловой плотности последовательности Λ. Обе эти функции определены для всех $0 \le \varphi \le \psi \le 2\pi$, кроме не более чем счётного (возможно, пустого) набора значений.

Теорема. *Пусть дана ограниченная выпуклая область $D \subset \mathbb{C}$ и правильно распределённая при порядке 1 последовательность $\Lambda \subset \mathbb{C}$, для которой $W_\Lambda(\varphi,\psi) = \frac{1}{2\pi} W_D(\varphi,\psi)$. Тогда существует такая система $\{e_{m,k}\}_{m=1,k=1}^{+\infty,N_m}$ экспоненциальных многочленов, что всякая функция $f(z) \in H(\overline{D})$ раскладывается в ряд вида*

$$f(z) = \sum_{m=1}^{+\infty} \sum_{k=1}^{N_m} d_{m,k} e_{m,k}(z),$$

сходящийся в $H(\overline{D})$.

Литература

1. Кривошеев А. С., Кривошеева О. А. *Базис в инвариантном подпространстве аналитических функций* // Матем. сб. – 2013. – Т. 204. – № 12. – С. 49–104.

2. Кривошеев А. С. *Базисы по „относительно малым группам”* // Уфимск. матем. журн. – 2010. – Т. 2. – №. 2. – С. 67–89.

3. Леонтьев А. Ф. *Ряды экспонент.* – М.: Наука, 1976. – 536 с.

4. Леонтьев А. Ф. *Целые функции. Ряды экспонент.* – М.: Наука, 1983. – 176 с.

5. Левин Б. Я. *Распределение корней целых функций.* – М.: ГИТТЛ, 1956. – 632 с.

EXPANDING FUNCTIONS HOLOMORPHIC IN BOUNDED CLOSED DOMAIN INTO SERIES BY A SYSTEM OF EXPONENTIAL POLYNOMIALS

A.I. Rafikov

This paper describes a particular case of expanding functions, holomorphic in a closed convex bounded domain, into a series of special exponential polynomials with properly distributed exponents sequence.

Keywords: interpolation, exponential polynomials, convex domain.

УДК 372.8

ИСПОЛЬЗОВАНИЕ ЭЛЕМЕНТОВ ИСТОРИИ МАТЕМАТИКИ В УЧЕБНОМ ПРОЦЕССЕ

З.З. Ризванов[1]

1 *rizvanov.zemfir@mail.ru*; Казанский (Приволжский) федеральный университет

Статья посвящена вопросам использования элементов истории математики в учебном процессе. Рассматриваются различные методы и формы введения исторического материала на уроках.

Ключевые слова: история математики, обучение, исторические сведения.

«*Тот, кто, обращаясь к старому,*
способен открывать новое, достоин быть учителем»
Конфуций

Современная школьная программа указывает на необходимость знакомства учеников с фактами из истории математики и биографиями великих математиков. Но в программе не уточняется, какую информацию из истории следует предоставлять ученикам, когда и как это делать. Ознакомление школьников с историей математики означает продуманное, систематическое знакомство на уроках с важнейшими событиями из истории науки в органической связи с систематическим изучением программного материала. Только такое тесное переплетение истории и теории обеспечит достижение этих целей.

Изучение истории математических структур, возникновения и формирования этих понятий, лежащих в их основе математических идей, позволяет сформировать представление о математике как целостной науке, развивающейся во взаимоотношениях ее отдельных областей. Школьники должны получить представление о том, как закладывались основания математики, какие фундаментальные знания были получены в различные исторические периоды.

Изучение истории математики знакомит учащихся с историей математической культуры, математических идей, оказывающих влияние на методы познания в различных областях науки. Исторический материал, действуя на сознание, чувства учеников, формирует их нравственные идеалы. Жизнь и деятельность многих ученых могут служить примером усердия и упорства в работе, веры в собственные силы. Кроме того, история математики является частью общей истории, поэтому без ее использования не удается сформировать целостный взгляд на развитие человеческого общества в историческом процессе становления и развития знания.

Таким образом, знакомство учащихся с фрагментами истории математики имеет определенные цели:

1) исторические экскурсы повышают интерес школьников к изучению предмета и углубляют понимание ими изучаемого раздела программы;

2) знакомство с историческими фактами расширяет кругозор, позволяет лучше понять роль математики в современном обществе;

3) сведения из истории побуждают учащихся к самостоятельной и творческой работе в математике;

4) они формируют представления об основных периодах развития математики как части человеческой культуры.

На первый взгляд кажется трудным найти на уроке время, необходимое для ознакомления с историческим материалом. Однако вопрос об использовании элементов истории математики на уроках практически полностью подчинен главному вопросу – связи изучаемой в школе математики с историей. Какой бы ни была форма сообщения исторических фактов – краткая беседа, экскурс, лаконичная справка, решение задачи, показ и разъяснение рисунка – использованное время нельзя считать потерянным напрасно, если учитель сумел преподнести исторический факт в тесной связи с изучаемым на уроке теории. Задания с элементами истории математики мотивируют изучение учебного материала. Например, одной из важнейших проблем преподавания математики в основной школе является проблема организации повторения в 5 классе. Необходимо, с одной стороны, обновить существующие знания учеников, с другой стороны, обогатить их. Кроме того, это повторение должно способствовать развитию общих интеллектуальных умений учащихся, создавать настрой на успех. Для повторения позиционных записей натуральных чисел могут быть использованы задачи, которые подчеркивают особенности этой формы представления натуральных чисел.

Так, например, «в римской» системе счисления используются цифры:

I – 1; V – 5; X – 10; L – 50; C – 100; D – 500; M – 1000.

Когда написано несколько римских цифр рядом, то число, обозначаемое ими, читается по следующим правилам:

1. Если цифра с большим значением стоит слева от цифры с меньшим значением, то их значения складываются.

2. Если цифра с меньшим значением стоит слева от цифры с большим значением, то из большего значения вычитается меньшее. При этом, меньшая цифра не должна повторяться.

3. Если рядом стоят две одинаковые цифры, то их значения складываются.

4. Одна и та же цифра может быть написана подряд не более трех раз.

Например, число 7 записывают VII (V + I + I); число 19 – XIX (X + X - I); число 174 = CXXIV; и наоборот, CXLVII = 100 + 40 + 5 + 1 +1 = 147.

Задания с элементами истории математики, способствуют развитию общих интеллектуальных умений, таких как умение решать проблемы. Практически по всем предметам школьного курса математики 5-6 классов целесообразно изучение старых задач.

Приведем одну из старинных задач. Некий человек нанял работника на год, обещав ему дать 12 руб. и кафтан. Но тот, отработав 7 месяцев, захотел уйти и просил достойной платы с кафтаном. Хозяин дал ему по достоинству расчет 5 руб. и кафтан. Спрашивается, а какой цены тот кафтан был?

Решение. Рассуждая логически, вычислим последовательно: работник не получил $12 - 5 = 7$ (руб.) за $12 - 7 = 5$ (месяцев), поэтому за один месяц ему платили $7 : 4 = 1,4$ (руб.), а за 7 месяцев он получил $7 * 1,4 = 9,8$ (руб.), тогда кафтан стоил $9,8 - 5 = 4,8$ (руб.).

Еще один пример (*древнеримская задача*). Один господин завещал капитал в 14 000 рублей своей жене при условии, что если у неё родится мальчик, то сын дол-

жен получить вдвое больше матери, а если родится дочь, то мать должна получить вдвое больше дочери. Родились близнецы: сын и дочь. Как было исполнено завещание?

Решение: Из наследства должна быть выделена одна часть матери, две такие же части сыну, а половина такой же части дочери. Все наследство должно быть разделено на $1+2+\frac{1}{2}=3\frac{1}{2}$ части. Одна часть составляет $14000:3\frac{1}{2}=4000$ рублей. Следовательно, мать должна получить 4000 рублей, сын 8000 рублей, дочь 2000 рублей.

Изучение курса алгебры в 7 классе можно начать с решения старинной задачи о кроликах и фазанах.

«Некто подошел к клетке, в которой сидели фазаны и кролики. Сначала он сосчитал головы, их оказалось 15. Потом он подсчитал лапки, их было 42. Сколько кроликов и сколько фазанов было в клетке?»

Задачу можно решить двумя способами – арифметическим и алгебраическим. Нужно рассмотреть с учениками два способа решения задачи и обсудить алгебраический способ, который служит мотивом для введения алгебраического языка.

Также с учениками 5-7 классов можно выполнять творческие и проектные работы: оформление стенгазеты, посвященной великим ученым-математикам; составление математических кроссвордов и чайнвордов; подготовка докладов и сообщений. Все это предоставляет богатейшие возможности для возбуждения творческих сил учащихся, укрепления их веры в собственные силы.

С учащимися старшей школы можно организовать конференции и интеллектуальные беседы на темы, связанные с историей математики: «Появление понятия функции», «Квадратичная функция» , «Известные женщины-математики», «Пять мифов о геометрии Лобачевского», «Тригонометрическая окружность», «Зарождение алгебры и геометрии», «Основы учения о числе в XVIII в. и начале XIX в.», «Казанские математики XX и XXI вв.» и т. д.

Таким образом, введение элементов истории математики на уроках необходимо в силу «внутренней историчности» всего курса математики. Исторические материалы позволяют школьникам пересмотреть изученное с другой точки зрения, отнестись к нему как к элементу культуры, увидеть развитие методов математики и человеческой мысли.

Литература

1. Глейзер Г. И. *История математики в школе. VII- VII кл. Пособие для учителей.* – М.: Просвещение, 1982. – 342 с.

2. Рыбников К. А., *Возникновение и развитие математической науки. Книга для учителя.* – М.: Просвещение, 1987. – 240 с.

3. Смолякова Д. В. *Учебные задания с элементами истории математики как средство обогащения умственного опыта учащихся основной школы при обучении математике* // Дисс … Новосибирск, 2006. – 171 с.

4. Чистяков В. Д., *Сборник старинных задач по элементарной математике с историческими экскурсами и подробными решениями*. – Минск, 1962.

5. Шакирова Л. Р. *Историзация математического образования в школе и вузе* // Матем. обр. в школе и вузе: теория и практика (MATHEDU - 2016): Материалы VI Межд. научно-практ. конф. (Казань, 25-26 ноября 2016 г.). – С. 297–307.

THE USE OF ELEMENTS OF HISTORY IN TEACHING MATHEMATICS

Z.Z. Rizvanov

The article is devoted to the use of elements of history of mathematics in the educational process. It discusses various methods and forms of introduction of the historical material in teaching mathematics.

Keywords: history of mathematics, teaching, historical information.

УДК 519.688, 511.174

СИЛОВСКИЕ ПОДГРУППЫ АТ-ГРУПП

А.В. Рожков[1], М.В. Рожкова[2]

1 *ros.seminar@bk.ru*; Кубанский государственный университет
2 *ros.seminar@bk.ru*; Краснодарский колледж управления, техники и технологий

Изучаются силовские подгруппы АТ-групп над последовательностью конечных циклических групп. Решен вопрос из Коуровской тетради.

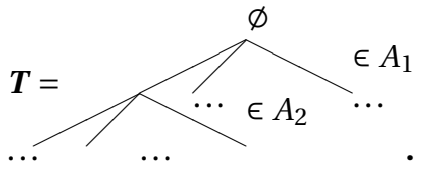
Ключевые слова: теория групп, пакеты компьютерной алгебры, силовские подгруппы, бернсайдовы группы, не локально конечные периодические группы.

Введение

Бернсайдовыми группами называются бесконечные конечно порожденные периодические группы. Первым примером бернсайдовой группы, заданной представлением, а не копредставлением, точнее, реализованной в виде конечного автомата, является конструкция С.В. Алешина [1]. В работе [2] конструкция Алешина была обобщена и введен класс АТ-групп (Aleshinsky type groups или, в более широком прочтении, automorphisms of trees groups).

Пусть $A = (A_1, A_2, \dots)$ — последовательность множеств, каждое из которых содержит не менее двух элементов. Наборы $u = (a_1, \dots, a_n)$, $a_i \in A_i$, будем называть кортежами длины n, $|u| = n$. Множество T всех кортежей превратим в дерево, соединяя ребрами вершины $u = (a_1, \dots, a_n)$ и $v = (a_1, \dots, a_n, a_{n+1})$, $n \in \mathbb{N}$. Бесконечный кортеж $\gamma = (a_1, a_2, ..., a_n, ...)$ назовем путем в дереве T.

Наглядно дерево T изображено на рисунке:



Всякий автоморфизм f дерева T, фиксирующий начальную вершину, однозначно задается набором перестановок ребер дерева T, размещенных в его вершинах: $f = \{f(u) \mid u \in T\}$, где $f(u)$ — перестановка множества $A_{|u|+1}$, размещенная в

вершине u. Перестановку $f(u)$ будем называть u-й, а если важна только длина n вершины u, то n-й сопровождающей перестановкой автоморфизма f.

Определение. *Автоморфизм f дерева T называется корневым, если $f(\emptyset)$ — единственная нетождественная сопровождающая перестановка автоморфизма f.*

Пусть γ — некоторый путь в дереве T. Автоморфизм f дерева T называется продольным, с направляющим путем γ, если из $f(u) \neq 1$ следует, что $u = (\gamma_1\gamma_2\dots\gamma_n a_{n+1})$, для некоторого $n \in \mathbf{N}$ и $a_{n+1} \in A_{n+1}$, причем $a_{n+1} \neq \gamma_{n+1}$.

Определение *AT*-группы. *Пусть F — некоторое множество корневых и продольных автоморфизмов дерева T. Группа $G = gr(F)$ называется AT-группой над последовательностью A, если группа перестановок $\Pi_n = gr(f(u) \mid f \in F, |u| = n)$ транзитивна на множестве A_{n+1} для любого $n \in \mathbb{N}$.*

Следует отметить, что любая AT-группа бесконечна и имеет тривиальный центр [2].

Пусть G — AT-группа над деревом T. Пусть далее, $u \in T, |u| = n$, — вершина и $st_G(u)$ — стабилизатор вершины u группы G. Тогда сужение $st_G(u)$ на поддерево T_u с начальной вершиной u, тоже является AT-группой, но над последовательностью $A_{(n)} = (A_{n+1}, A_{n+2}, \dots)$, а ее порождающим множеством будут "хвосты" продольных порождающих группы G. Мы назовем эту группу n-срезкой и обозначим G_n.

Важнейшим частным случаем AT-групп, наиболее доступным изучению, являются регулярные AT-группы.

Определение. *Если последовательность $A = (A_1, A_2, \dots)$ состоит из групп, а все сопровождающие перестановки $f(u)$ являются элементами регулярного представления соответствующих групп A_n, то такую AT-группу мы будем называть регулярной.*

Важнейшим и самым изученным подклассом регулярных AT-групп является класс AT_ω-групп.

Определение. *Пусть $\omega = (p_1, p_2, \dots)$ — последовательность простых чисел, тогда регулярная AT-группа над последовательностью циклических групп $A = (A_{p_1}, A_{p_2}, \dots)$ называется AT_ω-группой.*

Регулярные *AT*-группы над последовательностью конечных циклических групп

Следует отметить, что до настоящего времени ни в одной периодической AT-группе, не являющейся p-группой, не найдены силовские подгруппы. Были серьезные подозрения, что в классе периодических AT_ω-группой над ограниченной, но не постоянной последовательностью ω, все силовские подгруппы локально конечны. Поэтому в [3] был поставлен вопрос о силовских подгруппах в более широком классе AT-групп.

Вопрос 16.79. *Верно ли, что в любой конечно порожденной AT-группе над последовательностью циклических групп, порядки которых ограничены, все силовские подгруппы локально конечны?*

Однако, класс конечных циклических групп от циклических групп простого порядка отличается очень сильно. Принципиально важно, что циклическая группа простого порядка порождается любым неединичным элементом и это многое меняет.

Например, в случае последовательности конечных циклических групп A существует регулярная AT-группа G, которая содержит подгруппу F, которая является

AT-группой, но над последовательностью B, существенно отличной от последовательности A. В случае AT_ω-групп подобное в принципе невозможно!

Собственно, это замечание и решает судьбу вопроса 16.79.

Теорема. *Существует периодическая регулярная AT-группа над последовательностью циклических групп ограниченного порядка, не являющаяся p-группой, у которой есть не локально конечная силовская подгруппа. То есть, вопрос 16.79 решается отрицательно.*

Пример 1. *Пусть $G = gr(a, g)$ — регулярная AT-группа над последовательностью $A = (\mathbb{Z}_{10}, \mathbb{Z}_{10}...)$, где $\mathbb{Z}_{10} = \{0, 1, ..., 9\}$. Корневой порождающий реализует перестановку $a(\emptyset) = (0, 1, ..., 9)$, а продольный порождающий имеет направляющий путь $(0, 0, ...)$ и на всех слоях дерева имеет одну и ту же структуру, которая не очень точно, но интуитивно оправданно, может быть описана в обозначениях программирования*

$$g := (g, 1, a, 1, a^{-1}, 1, 1, 1, 1, 1),$$

где 1 означает тождественное преобразование. Тогда G — $\{2, 5\}-$группа, а ее подгруппа $F = gr(a^2, f^2)$ является бесконечной 5-группой.

Идея доказательства. Непосредственно вычисляются порядки следующих элементов $|ag| = 100, |a^2g| = 50, |a^5g| = 20$. Далее периодичность доказывается индукцией по слоговой длине, с использованием идеи [2]. Теперь положим $b = a^2, f = g^2$, тогда b — корневой порождающий порядка 5, который задает перестановку двух независимых подмножеств $(0, 2, 4, 6, 9)(1, 3, 5, 7, 9)$, а продольный порождающий может быть описан рекурсией

$$f := (f, 1, b, 1, b^{-1}, 1, 1, 1, 1, 1).$$

Если выделить вершины с номерами $\{0, 2, 4, 6, 8\}$, то на них продольный порождающий примет вид $f := (f, b, b^{-1}, 1, 1)$, а на остальных вершинах он будет действовать тождественно. Таким образом, подгруппу F можно интерпретировать как регулярную AT-группу над последовательностью $B = (\mathbb{Z}_5, \mathbb{Z}_5...)$, которая поэтому будет бесконечной 5-группой. Она, конечно, не является силовской 5-подгруппой группы G, но гарантирует, что силовская 5-подгруппа не локально конечна.

Все силовские 2-подгруппы группы G, возможно, локально конечны.

Пример 2. *Пусть $G = gr(a, g)$ — регулярная AT-группа над последовательностью $A = (\mathbb{Z}_{35}, \mathbb{Z}_{35}...)$, где $\mathbb{Z}_{35} = \{0, 1, ..., 34\}$. Корневой порождающий реализует перестановку $a(\emptyset) = (0, 1, ..., 34)$, а продольный порождающий имеет направляющий путь $(0, 0, ...)$ и на всех слоях дерева имеет одну и ту же структуру, которая может быть описана рекурсией*

$$g := (g, 1, 1, 1, 1, a, 1, a, 1, 1, a^{-1}, 1, 1, 1, a^{-1}, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1),$$

где 1 означает тождественное преобразование. Тогда G — $\{5, 7\}-$группа, а ее подгруппа $F = gr(b = a^5, f = g^5)$ является бесконечной 7-группой, подгруппа $H = gr(c = a^7, h = g^7)$ является бесконечной 5-группой.

Таким образом, в примере 2 есть не локально конечные и 5- и 7-силовские подгруппы.

Идея доказательства – та же, что и в примере 1:

продольный порождающий подгруппы F действует на вершинах из списка $\{0, 5, 10, 15, 20, 25, 30\}$ и имеет вид $f := (f, b, b^{-1}, 1, 1, 1, 1)$,

продольный порождающий подгруппы H действует на вершинах из списка $\{0, 7, 14, 21, 28\}$ и имеет вид $h := (h, c, c^{-1}, 1, 1)$.

Гипотеза. *Пусть последовательность ω ограничена и содержит как минимум два различных простых числа бесконечное число раз. Тогда все силовские подгруппы любой конечно порожденной периодической AT_ω–группы локально конечны.*

Литература

1. Алешин С. В *Конечные автоматы и проблема Бернсайда о периодических группах* // Матем. заметки. – 1972. – Т. 11, № 3. – с. 319–328.

2. Рожков А. В. *К теории групп алешинского типа* // Матем. заметки. – 1986. – Т. 40, № 5. – С. 572–589.

3. *Нерешенные вопросы теории групп. Коуровская тетрадь.* Изд. 18-е, доп., вкл. архив решенных задач. Сост.: В.Д. Мазуров, Е.И. Хухро. — Новосибирск: Институт математики, 2014. — 254 с.

SYLOW SUBGROUPS OF AT-GROUP

A.V. Rozhkov, M.V. Rozhkova

Sylow subgroups of AT-group over the sequence of finite cyclic groups are studied. A problem from the Kourovka notebook is resolved.

Keywords: group theory, packages of computer algebra, Sylow subgroups, Burnside groups, not locally finite torsion groups.

УДК 519.688, 511.174

НИЖНИЙ ЦЕНТРАЛЬНЫЙ РЯД *AT*-ГРУППЫ

А.В. Рожков[1], М.В. Рожкова[2]

1 *ros.seminar@bk.ru*; Кубанский государственный университет
2 *ros.seminar@bk.ru*; Краснодарский колледж управления, техники и технологий

Изучаются нижние центральные ряды AT-групп над последовательностью циклических групп простых порядков.

Ключевые слова: теория групп, пакеты компьютерной алгебры, нижний центральный ряд, бернсайдовы группы, не локально конечные периодические группы.

Введение

Бернсайдовыми группами называются бесконечные конечно порожденные периодические группы. Первым примером бернсайдовой группы неограниченного периода, заданной представлением, а не копредставлением, является конструкция С.В. Алешина [1]. В работе [2] конструкция Алешина была обобщена и введен класс AT-групп.

Все необходимые нам определения и обозначения приведены в работе А.В. Рожков, М.В. Рожкова и “Силовские подгруппы AT-групп”, публикуемой в этом же сборнике.

Основной объект нашего изучения – AT_ω-группы.

Определение. *Пусть $\omega = (p_1, p_2, \ldots)$ — последовательность простых чисел, тогда регулярная AT-группа над последовательностью циклических групп $A = (A_{p_1}, A_{p_2}, \ldots)$ называется AT_ω-группой.*

Также напомним определение нижнего центрального ряда группы. Отметим, что верхнего центрального ряда у AT-групп нет, поскольку они имеют единичный центр.

Определение. *Пусть G — группа. Второй член нижнего центрального ряда группы G — это коммутант $\gamma_2(G) = [G, G]$. Если n-й член $\gamma_n(G)$ нижнего центрального ряда уже определен, то $\gamma_{n+1}(G) = [\gamma_n(G), G]$.*

Нижний центральный ряд 2-группы Григорчука и 3-группы Гупты-Сидки

Вопрос о существовании группы с бесконечным нижним центральным рядом, все факторы которого ограничены в совокупности, приписывается филдсовскому лауреату Е.Зельманову и известному алгебраисту А.Шалеву. В любом случае, вопрос оказался очень трудным. В [3] впервые был вычислен нижний центральный ряд 2-группы Григорчука и выяснилось, что все его факторы имеют порядок 2 или 4.

Определение. *Группа Григорчука $G = gr(c, f, g, h)$ является AT_ω-группой над последовательностью $\omega = (2, 2, \ldots)$. При этом c — корневой порождающий, f, g, h — продольные порождающие с направляющим путем $(0, 0, \ldots)$, задаваемые рекурсивно $f := (g, c), g := (h, c), h := (f, 1)$. Таким образом, $c^2 = f^2 = g^2 = h^2 = 1, h = fg$, т.е. группа Григорчука порождается тремя инволюциями, две из которых перестановочны. Это – экстремально "экономное" порождающее множество.*

В пакете GAP4, официальный сайт `http://www.gap-system.org`, была создана программа, вычисляющая факторы нижнего центрального ряда группы Григорчука. Вычисленные первые несколько сотен факторов совпали с предсказанными в работе [3]. Здесь находится текст программы `http://www.gap-system.org/Doc/Examples/grigorchuk.html`.

Следуюшая попытка вычисления факторов была предпринята в работе [4] в отношении 3-группы Гупты-Сидки. Однако, несмотря на довольно значительный объем работы, удалось вычислить только первые 10 факторов нижнего центрального ряда.

Определение. *Группа Гупты - Сидки $G = gr(c, g)$ является AT_ω-группой над последовательностью $\omega = (3, 3, \ldots)$. При этом, c — корневой порождающий, g — продольный с направляющим путем $(0, 0, \ldots)$, задаваемый рекурсивно $g := (g, c, c^{-1})$. Таким образом, $c^3 = g^3 = 1$. Группа Гупты - Сидки самая просто задаваемая AT-группа.*

Оставшиеся проблемы

В работе [3] есть три существенных недочета, по-видимому устранимые.

Первое. В одной из основных лемм, описывающей некоторые коммутаторные тождества, не разобран один из случаев и, формально, лемма не доказана.

Второе. Индуктивное построение векторных пространств, возникающих при вычислении факторов нижнего центрального ряда, слишком лаконично и не может рассматриваться как полное и тем более исчерпывающее доказательство.

Третье. Идейно доказательство плохо проработано, поскольку не может быть применено к другим AT-группам.

Учитывая, что с 1996 г. прогресса по этой теме фактически нет и работа [3] остается единственной, доведенной до итогового результата, — вычисления всех факторов нижнего центрального ряда, имеет смыл вернуться к ней и устранить перечисленные недостатки.

Что нами и было предпринято. Исследования получились довольно обширными. Здесь мы не имеем возможности привести даже фрагменты построения этой системы векторных пространств, которые оказались интересными объектами даже с точки зрения их самостоятельного изучения. Полная работа готовится для журнальной публикации.

Литература

1. Алешин С.В. *Конечные автоматы и проблема Бернсайда о периодических группах* // Матем. заметки. – 1972. – Т. 11, № 3. – С. 319–328.

2. Рожков А.В. *К теории групп алешинского типа* // Матем. заметки. – 1986. – Т. 40, № 5. – С. 572–589.

3. Рожков А.В. *Нижний центральный ряд одной группы автоморфизмов деревьев* // Матем. заметки. – 1996. – Т. 60, № 2. – С. 225–237.

4. Vieira A.C. *On the lower central series and the derived series of the gupta-sidki 3-group* // Communications in Algebra. – 1998. – V. 26, № 4. – P. 1319–1333.

LOW CENTRAL SERIES OF AT-GROUP

A.V. Rozhkov, M.V. Rozhkova

The lower central series of AT-group over the sequence of cyclic groups of prime orders are studie.

Keywords: group theory, packages of computer algebra, low central series, Burnside groups, not locally finite torsion groups.

УДК 514.76

ОБ ОБЪЕКТЕ КРИВИЗНЫ ФУНДАМЕНТАЛЬНО-ГРУППОВОЙ СВЯЗНОСТИ 2-ГО ПОРЯДКА

Н.А. Рязанов[1]

1 *ryazanov-92@mail.ru*; Балтийский федеральный университет им. И. Канта, Институт физико-математических наук и информационных технологий

Объект кривизны 2-го порядка содержит объект кривизны фундаментально-групповой связности, задаваемой в главном расслоении; объект кривизны аффинной связности над многообразием; компоненты 2-го порядка. Выведены дифференциальные сравнения на компоненты объекта кривизны фундаментально-групповой связности 2-го порядка. Эти сравнения показывают, что объект кривизны 2-го порядка образует геометрический объект лишь в совокупности с компонентами 2-го порядка объекта связности. В общем случае объект кривизны фундаментально-групповой связности 2-го порядка не образует тензор.

Ключевые слова: структурные уравнения Лаптева, фундаментально-групповая связность, объект кривизны 2-го порядка.

Рассмотрим главное расслоение $G_r(M_n)$, базой которого служит n-мерное гладкое многообразие M_n, а типовым слоем является r-членная группа Ли G_r. Фундаментально-групповая связность 2-го порядка задается в продолженном главном расслоении со структурными уравнениями

$$D\omega^i = \omega^j \wedge \omega^i_j,\ \ D\omega^\alpha = C^\alpha_{\beta\gamma}\omega^\beta \wedge \omega^\gamma + \omega^i \wedge \omega^\alpha_i,\ \ D\omega^i_j = \omega^k_j \wedge \omega^i_k + \omega^k \wedge \omega^i_{jk},$$

$$D\omega^\alpha_i = \omega^j_i \wedge \omega^\alpha_j + \omega^\beta_i \wedge \omega^\alpha_\beta + \omega^j \wedge \omega^\alpha_{ij}\ \ (\omega^\alpha_\beta = C^\alpha_{\beta\gamma}\omega^\gamma,\ \ i,\ldots = \overline{1,n},\ \alpha,\ldots = \overline{n+1,n+r})$$

с помощью поля объекта $\Gamma^2 = \{\Gamma^\alpha_i, \Gamma^i_{jk}, L^\alpha_{ij}\}$, компоненты которого удовлетворяют дифференциальным уравнениям

$$\Delta\Gamma^\alpha_i + \omega^\alpha_i = \Gamma^\alpha_{ij}\omega^j,\ \ \Delta\Gamma^i_{jk} + \omega^i_{jk} = \Gamma^i_{jkl}\omega^l,\ \ \Delta L^\alpha_{ij} - C^\alpha_{\beta\gamma}\Gamma^\gamma_j\omega^\beta_i + \Gamma^k_{ij}\omega^\alpha_k + \omega^\alpha_{ij} = L^\alpha_{ijk}\omega^k.$$

Объект Γ^2 определяет формы связности

$$\Omega^\alpha = \omega^\alpha - \Gamma^\alpha_i\omega^i,\ \ \Omega^i_j = \omega^i_j - \Gamma^i_{jk}\omega^k,\ \ \Omega^\alpha_i = \omega^\alpha_i - L^\alpha_{ij}\omega^j,$$

удовлетворяющие структурным уравнениям

$$D\Omega^\alpha = C^\alpha_{\beta\gamma}\Omega^\beta \wedge \Omega^\gamma + R^\alpha_{ij}\omega^i \wedge \omega^j,\ \ D\Omega^i_j = \Omega^k_j \wedge \Omega^i_k + R^i_{jkl}\omega^k \wedge \omega^l,$$

$$D\Omega^\alpha_i = \Omega^j_i \wedge \Omega^\alpha_j + C^\alpha_{\beta\gamma}\Omega^\beta_i \wedge \Omega^\gamma + K^\alpha_{ijk}\omega^j \wedge \omega^k,$$

в которые входят компоненты 2-го порядка

$$K^\alpha_{ijk} = L^\alpha_{i[jk]} - \Gamma^l_{i[j}L^\alpha_{lk]} - C^\alpha_{\beta\gamma}L^\beta_{i[j}\Gamma^\gamma_{k]}$$

объекта кривизны фундаментально-групповой связности 2-го порядка. Эти компоненты удовлетворяют дифференциальным сравнениям

$$\Delta K^\alpha_{ijk} \cong L^\alpha_{il}\omega^l_{[jk]} - R^l_{ijk}\omega^\alpha_l + C^\alpha_{\beta\gamma}R^\gamma_{jk}\omega^\beta_i - \omega^\alpha_{i[jk]}\ (mod\ \omega^i).$$

Объект кривизны 2-го порядка $R^2 = \{R^\alpha_{ij}, R^i_{jkl}, K^\alpha_{ijk}\}$ содержит: а) объект кривизны R^α_{ij} фундаментально-групповой связности, задаваемой в главном расслоении $G_r(M_n)$, б) объект кривизны R^i_{jkl} аффинной связности над многообразием M_n, в) компоненты 2-го порядка K^α_{ijk}.

Объект кривизны R^2 образует геометрический объект лишь в совокупности с компонентами 2-го порядка L^α_{ij} объекта связности 2-го порядка Γ^2. В общем случае объект кривизны R^2 фундаментально-групповой связности 2-го порядка не образует тензор (см. [1, 2]).

Литература

1. Рязанов Н. А. *Дифференциальные сравнения компонент объекта кривизны аффинной связности 2-го порядка в несимметричном случае* // Диф. геом. многооб. фигур. – Калининград. – 2017. – Вып. 48. – С. 95–104.

2. Рыбников А. К. *Об аффинных связностях второго порядка* // Матем. заметки. – 1981. – Т. 29, Вып. 2. – С. 279–290.

ABOUT THE OBJECT OF CURVATURE OF A FUNDAMENTAL-GROUP CONNECTION OF THE 2ND ORDER

N.A. Ryazanov

The second-order curvature object contains the curvature object of the fundamental-group connection defined in the principal bundle; the curvature object of an affine connection over a manifold; second-order components. Differential comparisons for the components of the object of curvature of the second-order fundamental-group connection are made. These comparisons show that the curvature object of the second-order forms a geometric object only in combination with second-order components connectivity object. In the general case, the object of curvature of the fundamental group connection of the second order does not form a tensor.

Keywords: structure equations of Laptev; fundamental-group connection, the second order curvature object.

УДК 004.91

АЛГОРИТМ ИЗВЛЕЧЕНИЯ СВЯЗЕЙ В НАУЧНЫХ ЦИФРОВЫХ КОЛЛЕКЦИЯХ

Э.М. Сабитова[1]

1 *sabitovae441@gmail.com*; Казанский (Приволжский) федеральный университет, Институт математики и механики им. Н.И. Лобачевского

Работа посвящена извлечению семантических связей в научных цифровых коллекциях. Исследованы свойства и типы связей, рассмотрены существующие алгоритмы извлечения связей в цифровых коллекциях научных документов. Предложен алгоритм извлечения связей между авторами в виде совместной публикации.

Ключевые слова: семантическая связь, онтология, алгоритм *k* ближайших соседей.

На сегодняшний день текстовая аналитика является одним из главных направлений разработок информационных технологий, а структурирование информации, описанной на естественном языке, и извлечение из нее связей – одной из важных задач современного общества. Одной из особенностей естественного языка является возможность представления одной информации разными способами даже на одном определенном языке. Естественным образом возникает необходимость некоторого единого представления и структурирования данного исходного неструктурированного текста. Как только информация, представленная в тексте, становится упорядоченной и привязанной к некоторой системе идентификаторов, появляется возможность для автоматической работы с ней: извлечения связей, поиска нужной информации, поиска похожих текстов и прочих задач обработки текста. В работе мы рассмотрели задачу извлечения связей.

В нашей работе *семантическая связь* – это некая универсальная связь, усматриваемая носителем языка в тексте, то есть это связь слова с другими словами, входящими вместе с ним в одну семантическую систему [1], [2].

Связи бывают двух типов:

- иерархические (образуют древовидную структуру);

- вспомогательные (логические, атрибутивные, функциональные, количественные, пространственно-временные, лингвистические).

Также отношения обладают следующими свойствами: наличие обратного отношения, симметричность отношения и транзитивность отношения.

В качестве более ясного представления алгоритмов извлечения связей рассмотрим алгоритмы *k* ближайших соседей (*k*-Nearest Neighbors algorithm – kNN), модифицированный алгоритм *k* ближайших соседей (Modified *k*-Nearest Neighbors – MKNN), алгоритм, основанный на онтологии, алгоритм, использующий шаблоны.

- Работа алгоритмов KNN и MKNN состоит в следующем [3]. Для начала вычисляется мера семантической близости всех возможных пар определений. На основе вычислений заполняется массив наиболее близких слов для каждого определения. При этом число элементов этого массива поддерживается равным *k* (*k* – количество ближайших соседей); это позволяет сократить потребление памяти без потери информации о связности слов. После заполнения массива для получения результирующего набора отношений *R* необходимо в методе KNN — заполнить выходное множество, для метода MKNN – дополнительно проверить для каждого определения его вхождение в массив наиболее близких слов, и если входит — добавить его в результирующее множество.

- Алгоритм, основанный на онтологии.

  Онтология представляет собой формализацию некоторой области знаний при помощи концептуальной схемы (информация представляется как иерархическая структура понятий). Такая схема включает в себя описание понятий, их свойств, отношений между ними и некоторой логики (набора правил, теорем, ограничений), ограничивающей возможные свойства и отношения для различных понятий.

  Онтологии используются для формальной спецификации понятий и отношений, которые характеризуют определенную область знаний [4], [5]. Так как компьютер не может понимать положение вещей в мире так, как человек, ему необходимо представление всей информации в формальном виде. Онтологии снабжают систему сведениями о хорошо описанной семантике заданных слов и указывают иерархическое строение области, взаимосвязь элементов. Все это позволяет компьютерным программам при помощи онтологий делать умозаключения из представленной информации и манипулировать ими.

- Алгоритм, основанный на шаблонах.

  В данном алгоритме каждое предложение, которое поступает на вход, постепенно сокращается: некоторые части предложения согласно правилам, которые описаны в шаблонах, добавляются в очередь с приоритетом, после на каждом шаге алгоритма из поступившего на вход предложения отбирается та часть, которая имеет в очереди наибольший приоритет. Для определения приоритета в такой очереди используются два значения: значение приоритета группы, к которой принадлежит связь, описанная в шаблоне, и позиция слова в предложении.

На основе определений «семантическая связь», свойств и типов связей, а также существующих алгоритмов мы предложили достаточно простой алгоритм выявления связей между авторами в виде публикаций.

Для этого был создан специальный XML – язык, содержащий в себе данные определенной научной коллекции. В рамках эксперимента нами была использованы статьи, написанные преподавателями Института математики и механики им. Н.И Лобачевского Казанского федерального университета. Созданный XML язык представляет собой набор тегов, описывающих публикации и работы коллекции. Таким образов в тег описания работы <book> включены следующие теги: <authors> – содержит в себе перечисление всех авторов (<author>) описываемой публикации, <title> – название публикации, <year> – год ее опубликования, <pub> – ВУЗ, в издательстве которого она опубликована. <URL> – актуальные ссылки для свободного скачивания публикаций. Следующим этапом является создание веб-приложения на языке PHP. Интерфейс приложения представляет собой веб-формы, в которые будем вводить фамилию, имя и отчество искомых авторов, кнопку, с помощью которой можно добавлять авторов, и кнопку, при нажатии которой программа будет осуществлять поиск связей между введёнными авторами. При нажатии поиска происходит процесс считывания информации из отправленного файла, то есть из формы, производится разделение на фамилию, имя и отчество. Программа выясняет какие статьи были написаны первым автором, ищет совпадения с документами второго автора, если же число авторов n, то цикл будет продолжаться n раз. При окончании цикла, программа выводит результат в виде таблицы, в которой будут представлены данные, прописанные в описании публикации.

Работа выполнена за счет средств субсидии, выделенной Казанскому федеральному университету для выполнения государственного задания в сфере научной деятельности, проект 1.2368.2017/ПЧ, и при частичной финансовой поддержке РФФИ и Правительства Республики Татарстан в рамках научного проекта №15-47-02472.

Литература

1. Мочалова А. В. *Алгоритм семантического анализа текста, основанный на базовых семантических шаблонах с удалением* // Научно-техн. вестн. инф. техн., механики и оптики. – 2014. – № 5(93). – С. 126–132.

2. Когаловский М.Р., Паринов С.И. *Научные коммуникации на базе электронных библиотек с онлайновой декларацией семантических связей* // CEUR-Workshop Proceedings. — 2014. — V. 1297. — P. 81–89.

3. Панченко А. И., Адейкин С. А., Романов А. В., Романов П. В. *Извлечение семантических отношений из статей Википедии С помощью алгоритмов ближайших соседей* // Открытые системы. – 2012. – № 16. – С. 18–27.

4. Elizarov A., Kirilovich A., Lipachev E., Nevzorova O. *Mathematical knowledge management: ontological models and digital technology* // CEUR Workshop Proceedings. 2016. – V. 1752. – P. 44–50.

5. Elizarov A., Kirillovich A., Lipachev E., and Nevzorova O. *Digital ecosystem ontoMath: mathematical knowledge analytics and management* // Comm. in Comp. and Inf. Science, Springer. – 2017. – V. 706. – P. 33–46.

ALGORITHM OF RELATION EXTRACTION IN SCIENTIFIC DIGITAL COLLECTIONS

E.M. Sabitova

The article examines the topic of extracting semantic relation in scientific digital collections, studies the properties and typed links, considers the existing algorithms for extracting links. An algorithm for extracting links between authors in the form of a joint publication is proposed.

Keywords: semantic relation, ontology, k–Nearest Neighbors algorithm.

УДК 66.011

АСИМПТОТИЧЕСКОЕ РАЗЛОЖЕНИЕ РЕШЕНИЯ ЗАДАЧИ СВЕРХКРИТИЧЕСКОЙ ФЛЮИДНОЙ ЭКСТРАКЦИИ В ПОЛИДИСПЕРСНОМ СЛОЕ ВЫСОКОМАСЛИЧНОГО РАСТИТЕЛЬНОГО СЫРЬЯ

А.А. Саламатин[1]

1 *arthouse131@rambler.ru*; Казанский (Приволжский) федеральный университет

Получено асимптотическое разложения решения уравнений, описывающих динамику сверхкритической флюидной экстракции в полидисперсных слоях молотого растительного сырья. Выписаны первые три члена ряда, позволяющие с высокой точностью предсказывать динамику экстракции. Фракционный состав характеризуется тремя параметрами: объемной долей частиц мелкодисперсной фракции, удельной поверхностью и параметром полидисперсности частиц основной, крупнодисперсной фракции.

Ключевые слова: сверхкритическая флюидная экстракция, модель сужающегося ядра, асимптотическое разложение, функция распределения, полидисперсность.

Задача интерпретации экспериментальных данных и соответствующая параметризация моделей процесса — одна из актуальных проблем изучения сверхкритической флюидной экстракции (СФЭ) целевых соединений (масла) в полидисперсных пористых зернистых слоях молотого растительного сырья. В настоящее время для этих целей создано большое количество математических моделей. Детализация процесса для случая высокомасличного сырья в макромасштабном приближении (на уровне зернистого слоя), как правило, ограничивается учетом конвективно-фильтрационного выноса экстрагированных веществ из аппарата [1]. Межфазный массообмен определяется микромасштабной подмоделью диффузии масла в частицах сырья. В данной работе предполагается сферическая форма частиц и применяется модель сужающегося ядра (shrinking core — SC) [2, 3].

Набор параметров полной модели состоит из эффективного коэффициента диффузии D, определяющего интенсивность транспорта экстрагируемых веществ внутри частиц, и фракционного состава зернистого слоя. Последний обычно характеризуется плотностью $f(\xi)$ функции объемного распределения частиц по нормированным размерам (радиусам) ξ. Типичным для реальных экспериментов является существование двух ярковыраженных мод в области малых ($\xi < 1$) и больших ($\xi \gg 1$) размеров частиц. Эти фракции будем называть соответственно мелкодисперсной и крупнодисперсной (основной). Соответствующие функции распределения являются бимодальными, тот же термин будем применять в отношении соот-

ветствующих зернистых слоев [4]. Таким образом, плотность f можно записать в виде

$$f(\xi) = \alpha f_1(\xi) + (1-\alpha) f_2(\xi), \tag{1}$$

где α — объемная доля мелкодисперсной фракции, f_1 и f_2 соответственно – плотности распределений мелко- и крупнодисперсной фракций, а характерные значения ξ много меньше или много больше единицы.

Решение задачи СФЭ для произвольной f получено в квадратурах [5] относительно кривой $0 \le Y(\tau) \le 1$ выхода масла (КВМ) — доли масла, извлеченного из аппарата к моменту безразмерного времени τ. Типичным для КВМ является наличие начального участка линейного роста (с единичным наклоном) в течение времени τ_-, на котором в основном истощаются частицы мелкодисперсной фракции. Далее следует продолжительный этап нелинейного роста, во время которого масло содержится лишь в частицах основной фракции. В безразмерных переменных при $\tau > \tau_-$ решение удобно представить в следующем виде

$$1 \equiv \int_{\tau - Y(\tau)}^{\tau} \frac{d\tau}{k(\tau)}, \quad k(\tau) = \int_0^{\infty} s\left(\frac{\tau}{\xi^2}\right) f(\xi)\, d\xi, \tag{2}$$

$$3\left(1 - (1 - s(\omega))^{2/3}\right) - 2s(\omega) = \min\{1, \omega\}, \tag{3}$$

где функция истощения $0 \le s \le 1$ равна доле масла, извлеченного из частицы.

Учитывая представление (1) для плотности f, получим асимптотическое разложение решения (2)–(3)

$$\tau_- = \alpha + \frac{2}{\sqrt{3}} \frac{(1-\alpha)\alpha^{1/2}}{\xi_0} + \frac{1-\alpha}{2\xi_0^2}\left(1 - \alpha - \frac{2}{3}\Omega\alpha\right) + O(\xi_0^{-3}), \tag{4}$$

$$\begin{aligned} Y(\tau) = {} & \alpha + \frac{2}{\sqrt{3}} \frac{1-\alpha}{\xi_0 \alpha}\left(\tau^{3/2} - (\tau - \alpha)^{3/2}\right) - \\ & \frac{1}{\xi_0^2} \frac{1-\alpha}{6\alpha^2}\Big(2\alpha^2\Omega(2\tau - \alpha) + 3(1-\alpha)(\alpha^2 - 2\alpha\tau + 4\tau^2) + \\ & 12\tau^{3/2}(1-\alpha)\sqrt{\tau - \alpha}\Big) + O(\xi_0^{-3}), \quad \tau > \tau_- \end{aligned} \tag{5}$$

по малому параметру

$$\xi_0^{-1} = \int_0^{+\infty} \frac{f_2(\xi)}{\xi} d\xi \ll 1,$$

который имеет смысл удельной поверхности крупнодисперсной фракции. Параметр полидисперсности

$$\Omega = \int_0^{+\infty} \frac{\xi_0^2}{\xi^2} f_2(\xi)\, d\xi = O(1)$$

характеризует дисперсию плотности f_2 и равен единице, когда крупнодисперсная фракция представлена частицами лишь одного размера, а ее плотность выражается через δ-функцию Дирака, $f_2 = \delta(\xi - \xi_0)$.

Очередной член разложения содержит все больше параметров и уточняет информацию о кривой выхода масла. Нулевое приближение, отвечающее слагаемым порядка единицы в разложении (4)–(5), получается, если полностью пренебречь

массоотдачей крупной фракции. Следующее приближение учитывает проникновение фронта истощения по схеме SC вглубь частиц крупнодисперсной фракции на небольшую глубину по сравнению с их размерами. Кривизна поверхности раздела внутри частиц меняется слабо, оставаясь фактически постоянной. И, наконец, последнее слагаемое характеризует изменение кривизны фронта при его движении вглубь частиц. Однако, в зависимости от радиуса частиц кривизна изменяется с разной скоростью, и необходимо учитывать не только форму частиц, но и дисперсию их размеров. По этой причине в задаче появляется параметр полидисперсности Ω.

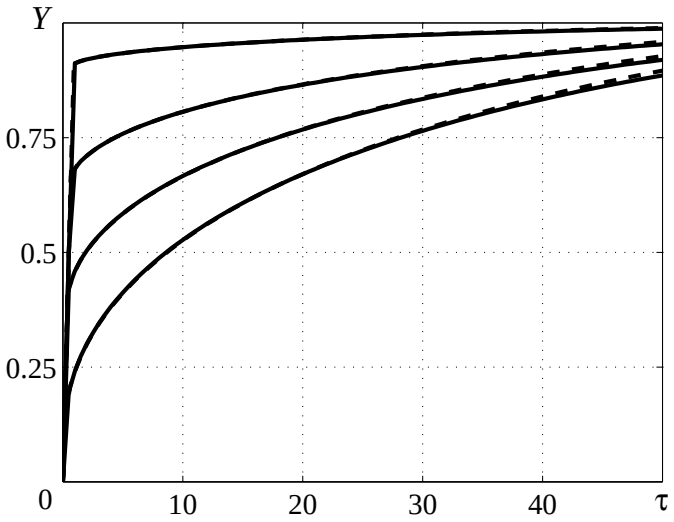


Рис. 1. Соответствие точного решения (сплошные линии) и приближенного (пунктирные линии), построенного по формулам (2)–(3) при $\Omega = 1$, $\xi_0 = 10$. Кривые отвечают разным α из интервала $[0.1; 0.9]$ с постоянным шагом.

Дальнейший смысл параметров ξ_0 и Ω раскрывается, если задаться конкретным классом распределений частиц по размерам. Данные лабораторных измерений позволяют остановиться на логнормальном распределении [1]

$$f_2(\xi) = \frac{1}{\sigma\sqrt{2\pi}\xi}\exp\left(-\frac{\log\xi - \mu}{2\sigma^2}\right).$$

В таком случае параметры Ω и дисперсия распределения σ, а также удельная поверхность и среднее μ связаны взаимнооднозначными соотношениями:

$$\Omega = \exp(\sigma^2), \quad \xi_0^{-1} = \sqrt{\Omega}e^{-\mu}.$$

Как следует из рис. 1, первых трех членов разложения вполне достаточно, чтобы с высокой точностью моделировать экстракцию в бимодальных зернистых слоях.

Таким образом, показано, что фракционный состав зернистого слоя достаточно характеризовать тремя параметрами, а именно объемной долей α частиц мелкодисперсной фракции (нулевого размера), удельной поверхностью ξ_0^{-1} и параметром полидисперсноти Ω крупнодисперсной фракции. Последние два параметра допускают интерпретацию в терминах среднего и дисперсии логнорамального распределения.

Работа выполнена при финансовой поддержке Академии Наук Республики Татарстан и РФФИ (проект 15-41-02542 р_поволжье_а).

Литература

1. Egorov A. G., Salamatin A. A. *Bidisperse shrinking core model for supercritical fluid extraction* // Chem. Eng. Technol. – 2015. – V. 38. – № 7. – P. 1203–1211.

2. Максудов Р. Н., Егоров А Г., Мазо А. Б. и др. *Математическая модель экстрагирования семян масличных культур сверхкритическим диоксидом углерода* // Сверхкрит. флюиды: теория и практика. – 2008. – Т. 3. – № 2. – С. 20–32.

3. Salamatin A. A. *Detection of micro-scale mass-transport regimes in supercritical fluid extraction* // Chem. Eng. Technol. – 2017. – V. 40. – № 5. – P. 829–837.

4. Егоров А Г., Саламатин А. А., Максудов Р. Н. *Прямые и обратные задачи сверхкритической экстракции из полидисперсного слоя растительного сырья* // Теор. основы хим. технол. – 2014. – Т. 48. – № 1. – С. 43–51.

5. Егоров А Г., Саламатин А. А. *Оптимизационные задачи в теории сверхкритической флюидной экстракции масла* // Изв. вузов. Математика. – 2015. – Т. 59. – № 2. – С. 59–69.

ASYMPTOTIC EXPANSION OF THE MODEL SOLUTION FOR THE SUPERCRITICAL FLUID EXTRACTION IN POLYDISPERSE PACKED BEDS

A.A. Salamatin

Asymptotic expansion of the model solution for the supercritical fluid extraction in polydisperse packed beds of ground plant material is derived. The first three terms of the expansion are obtained. They describe the simulation of extraction process with high accuracy. Fractional composition of polydisperse particles is described by three the parameters: volume fraction of small particles, specific surface area, and polydispersity parameter of main particle fraction of relatively large characteristic size.

Keywords: supercritical fluid extraction, shrinking core model, asymptotic expansion, distribution function, polydispersity.

УДК 51

РАЗВИТИЕ МАТЕМАТИЧЕСКОГО ОБРАЗОВАНИЯ НА КУБАНИ И КАЗАНСКАЯ МАТЕМАТИЧЕСКАЯ ШКОЛА

Д.А. Сверкунова[1], А.С. Черная[2]

1 *belosnegka97@mail.ru*; Кубанский государственный университет
2 *chernaya-nastya@icloud.com*; Кубанский государственный университет

В статье обсуждается прямое влияние Казанской математической школы на развитие математики и математического образования на Кубани.Рассказывается о создании лицея №4 г. Краснодара по образцу СОШ № 131 г. Казани.

Ключевые слова: социальный капитал, математические школы, развитие математики на Кубани.

В 60-70 г. прошлого столетия многие педагогические институты СССР были преобразованы в университеты. Новая история Кубанского государственного университета началась в 1970 году. Одновременно возникали новые проблемы: научно-педагогические кадры, оснащение лабораторий, создание вычислительных центров, обеспечение жилплощадью новых сотрудников и др. Каждый регион решал

эти проблемы по-своему, но находилось и нечто общее, например, имеющиеся научные и деловые контакты, личные связи, доверительное отношение между коллегами, т. е. использование социального капитала или социальных связей и социальных сетей для достижения экономических, научных и образовательных целей. Между КубГУ и Казанским университетом сложились особые отношения благодаря конкретным личным контактам и общими научными интересами выпускников физмата, мехмата и факультета вычислительной математики Казанского государственного университета, особой атмосфере в среде мехматовцев тех лет и особой университетской культуре. Именно этот социальный капитал и был основой для развития научно-образовательных контактов между университетами.

Отметим, что способность к накоплению социального капитала не является индивидуальной характеристикой только одной личности, она является особенностью той сети отношений, которую выстраивают контактирующие. Таким образом, социальный капитал можно рассматривать как продукт включенности человека в социальную среду. Социальный капитал, сформированный в эти годы в казанской математической школе явился продуктом особого типа профессионального образования, когда профессиональное образование – не просто передача определенных знаний, методик и фактов, а процесс обучения моральным нормам, межличностным отношениям, ответственности, этическим принципам.

Прямое влияние на развитие математики и математического образования на Кубани оказали выпускники физмата и мехмата Казанского университета: З.Б. Цалюк и В.А. Лазарев, И.И. Ефремов и М.И. Дроботенко. Зиновий Борисович Цалюк(выпускник Казанского университета 1953 г.) был приглашен на работу ректором Краснодарского госпединститута в 1966 г. для активизации научной работы на физико-математическом факультете. В 1970 г. при реорганизации пединститута в Кубанский государственный университет образовалась кафедра дифференциальных уравнений, он многие годы был ее заведующим. За годы работы им подготовлено около 40 аспирантов. З.Б. Цалюк – крупный учёный, ведущий специалист по дифференциальным уравнениям (уравнения Вольтерра). Диапазон его исследований достаточно широк: ему принадлежат работы по функциональному анализу, дифференциальным уравнениям и уравнениям с запаздывающим аргументом, численным методам. Им опубликовано более 150 научных работ. С 1967 г. З.Б. Цалюк руководит организованным им научным семинаром по интегральным уравнениям, в работе которого принимают участие и ученые из других вузов, является членом ряда редколлегий научных изданий. Его ученики (В.Ф. Пуляев, и др.) работали и работают не только на математическом факультете, но и на других факультетах КубГУ и в вузах города и края. Зиновий Борисович много сил и энергии отдаёт становлению и развитию математического факультета Кубгу, внедряя лучшие традиции. Профессор З.Б. Цалюк – опытный педагог. Им разработаны учебные курсы по математическому анализу, функциональному анализу, дифференциальным уравнениям и методам вычислений. Он стал заслуженным профессором КубГУ. Многочисленные ученики Зиновия Борисовича ценили и ценят его талант, научно обоснованные четкие, и в то же время доступные и глубокие, объяснения сложного материала.

Виктор Андреевич Лазарев (выпускник Казанского университета 1965 г.) – док-

тор педагогических наук, кандидат физико-математических наук, профессор, заведующий кафедрой теории функций, лауреат премии Правительства РФ в области образования (2012 г.). После окончания университета В.А. Лазарев учился в аспирантуре и работал в НИИММ им. Н.Г. Чеботарёва, где и проявились черты способного исследователя и организатора. С 1970 года, с некоторыми перерывами, он связан с кафедрой теории функций КубГУ, с 1978 по 1981г. – декан математического факультета, одновременно заведующий кафедрой общей математики. Будучи заведующим кафедрой и деканом В.А. Лазарев открывает новые направления взаимодействия между казанскими математиками и механиками и математиками Кубани, многие казанские профессора приглашаются для чтения лекций (доктора наук О.М. Киселёв, М.А. Пудовкин, Ж.М. Сахабутдинов, Ш.У. Галиев). Регулярно в качестве председателей ГЭК из Казани приглашаются сотрудники НИИММ и мехмата КГУ, выпускники физмата Казанского университета (профессора А.В. Кузнецов, Л.М. Котляр, Л.А. Аксентьев, А.Д. Ляшко, академик В.Н. Монахов). Многие математики и механики КГУ выступают членами оргкомитетов школ и конференций по геометрической теории функций, организуемых на Черноморском побережье (Л.А. Аксентьев, Н.Б. Ильинский, Ф.Г. Авхадиев, Н.Б. Салимов, Е.Г. Шешуков, А.А. Назипов). Лучшие студенты Кубгу (М.И. Дроботенко, А.Г. Егоров) командируются для продолжения обучения в Казань.

В это же время на Кубани развивается система работы с одаренными школьниками, в Краснодаре открывается в 1984 году специализированная математическая школа (СШ №4) по образцу 131-й школы г. Казани. Начинают работать летние и зимние математические школы, усиливается работа ЮМШ, ВЗМШ. Многочисленные идеи, подхваченные в атмосфере математиков и механиков Казанского университета, реализуются на Кубани и играют важную роль в развитии математики в Кубанском университете, и главное – в повышении роли математики на Кубани За работу по поиску и поддержке одаренных школьников Виктор Андреевич Лазарев и его коллеги были удостоены Премии Комсомола Кубани в области педагогики в 1990 году.

Ион Иванович Ефремов (выпускник Казанского университета 1962 г.) – доктор физико-математических наук, профессор. Сначала (1980-1982) И.И. Ефремов заведовал кафедрой математического моделирования в Кубанском университете, затем (1989-1998) руководил кафедрой гидравлики в Кубанском аграрном университете. Ион Иванович известный специалист по гидродинамике крыла и численным методам подготовил из выпускников факультета прикладной математики специалистов по численным методам решения нелинейных задач гидродинамики. Это кандидаты физико-математических наук: Е.П. Лукащик, О.В. Гаркуша, С.В. Юнов, О.В. Иванисова, Н.М. Хуако)

Михаил Иванович Дроботенко (выпускник Казанского университета 1981 г.) – кандидат физ.-мат. наук, доцент, заведующий кафедрой математических и компьютерных методов КубГУ. Студент факультета прикладной математики Кубгу М.И. Дроботенко в 1979 г. был направлен в Казанский университет на кафедру вычислительной математики для завершения обучения, где успешно защитил диплом, а затем кандидатскую диссертацию. Вернувшись в Кубгу М.И. Дроботенко работает над численными методами математической физики, получает гранты, рабо-

тая с микробиологами, биофизиками, занимается робототехникой. Он ведёт плодотворную педагогическую деятельность, готовит магистрантов и аспирантов.

Андрей Геннадьевич Егоров (выпускник Казанского университета, 1980 г.) – заведующий кафедрой, заведующий отделением механики НИИММ им. Н.Г. Чеботарева, в КГУ получил ученые степени кандидата (1986) и доктора физико-математических наук (2000). Но ранее студент Андрей Егоров из Краснодара был направлен в Казанский университет завершить обучение и вернуться в Краснодар. Специальность Андрея Геннадьевича – механика жидкости, газа и плазмы. Работает в КГУ с 1982 года. Область его научных интересов: механика пористых сред.

Зоя Алексеевна Дегтярева закончила Казанский университет, научно-педагогическое отделение. Учитель-методист – отличник народного просвещения, заслуженный учитель Кубани, Соровский учитель, Зоя Алексеевна за свой многолетний труд в 2001 году награждена медалью «За выдающийся вклад в развитие Кубани II степени». С 1991 года преподает математику в школе-лицее № 90. Ее любят и уважают ученики за ее доброту, умение объяснить материал, терпение, полную отдачу себя ученикам. Результативность ее работы как учителя высока: большое количество призовых мест в окружных и городских олимпиадах, наличие участников Российской олимпиады, высокий процент поступления в вузы на математические и экономические специальности и др. Муж Зои Алексеевны, Дегтярев Александр Тимофеевич, также выпускник мехмата КГУ, многие годы преподавал в агроуниверситете г. Краснодара.

Мы здесь остановились только на нескольких выпускниках, математиках и механиках Казанского университета, активно работающих в Краснодаре в системе высшего и среднего образования 60–80–х годов, которые тесно взаимодействовали друг с другом и математическими школами Казани, тогда как затронутая тема вызывает необходимость отметить ещё небольшой «десант» казанских математиков и механиков, прибывших в Краснодар несколько раньше. В 1964 г в качестве сотрудников Краснодарского филиала научно-исследовательского института нефти и газа были приглашены из Казанского университета специалисты в области математического моделирования разработки нефтяных месторождений Д.Х. Динмухаметов, Н.В. Зубов, З.К. Хайрутдинов Руководство математического факультета Кубанского университета в 70-е годы установило с ними деловое научное сотрудничество, приглашая на преподавательскую деятельность и руководство дипломными работами.

Отметим ещё одну сферу сотрудничества математиков двух университетов. В 1961 году, при КГУ, открылась школа № 131 с углубленным изучением математики и физики. С ноября 2009 года – МАОУ «Лицей № 131» г. Казани. Целями обучения и воспитания в лицее являются: получение обучающимися полноценного среднего образования, развитие их интеллектуального потенциала и творческих способностей; достижение обучающимися высокого уровня развития, воспитание нравственной личности, руководствующейся общечеловеческими ценностями; профориентация и допрофессиональная подготовка учащихся в вузы с естественно-математической ориентацией. Школа в свое время находилась под патронажем ректора Казанского университета М.Т. Нужина, непосредственное кураторство осуществляли профессор М.А. Пудовкин и с.н.с. Р.И. Нигматуллин и др. работники университета. В качестве практиканта, будучи аспирантом Казанского

университета, несколько занятий в этой школе проводил В.А. Лазарев. В 1984 г., уже будучи заведующий кафедрой общей математики КубГУ, он вместе с директором СОШ №4 Краснодара Л.М. Куценко ездили в Казань для детального знакомства с работой школы № 131 Казани. Именно это знакомство с опытом работы казанской школы № 131 послужило основой открытия в Краснодаре в 1984 г. специализированных математических классов в СОШ №4. Ее определили в качестве базовой для математического факультета Кубанского университета, создали кабинет вычислительной техники, собрали ребят, увлекающихся математикой со всего Краснодара и занимались с ними по специальной программе.

Отдельные занятия в базовой, теперь уже физико-математической школе Кубанского университета начали вести преподаватели математического факультета, а практические занятия на ЭВМ проходили в вычислительной лаборатории КубГУ. Ученикам спецклассов прививалась работоспособность, активность на уроках. В процессе обучения у школьников вырабатывается устойчивое внимание, они приучаются логически мыслить, контролировать свои знания, учатся мыслить нестандартно, что очень ценно при решении задач, ищут разные способы решения, анализируют их, также пишут рефераты, выступают с докладами, учатся в заочных школах при МГУ и физико-техническом институте, ЮМШ при Кубанском университете, принимают участие в олимпиадах различного уровня, занимая призовые места. В те годы в течении трёх лет в специализированном классе занятия по математике вёл доцент В.А. Гусаков, т.е. многие процессы шли по образцу казанской СОШ № 131.

Изложенный выше материал показывает нам о возможностях создания деловых взаимовыгодных отношений в научно-образовательной сфере и реализации отдельных проектов при соответствующих условиях. Конечно, условия меняются, но есть (или могут быть) и инварианты, относящиеся к социальному, человеческому и интеллектуальному капиталам, что позволяет достигать результатов. Безусловно, выпускники Казанского университета сделали весомый вклад в развитие математики на Кубани, именно это мы и хотели показать. Подразумевается вклад и через достижения и успехи их учеников, которые пока не отражены в этой работе. Но эти успехи жизненно важны для нашей страны, для Кубани и конкретных людей. Перенимая опыт друг у друга, мы лучше будем способствовать развитию интеллектуальных, математических, творчески способностей и достигать нужных целей.

DEVELOPMENT OF MATHEMATICAL EDUCATION IN THE KUBAN AND KAZAN MATHEMATICAL SCHOOL

D.A. Sverkynova, A.S. Chernaya

The article discusses direct influence of the Kazan mathematical school on the development of mathematics and mathematical education in the Kuban.

Keywords: social capital, school of mathematics, development of mathematics in the Kuban.

УДК 512.556

ИЗОМОРФИЗМЫ РЕШЕТОК ПОДАЛГЕБР ПОЛУПОЛЕЙ НЕПРЕРЫВНЫХ ПОЛОЖИТЕЛЬНЫХ ФУНКЦИЙ С MAX-СЛОЖЕНИЕМ

В.В. Сидоров[1]

1 *sedoy_vadim@mail.ru*; Вятский государственный университет

Описаны изоморфизмы решеток подалгебр полуполей непрерывных положительных функций.

Ключевые слова: полуполе непрерывных функций, решетка подалгебр, изоморфизм, хьюиттовское пространство.

Данная работа является естественным продолжением статьи [1]; введение к [1] служит введением ко всей работе и содержит основные идейные предпосылки исследования. Напомним несколько понятий и обозначений; за недостающими отсылаем к [1].

Полукольцом называется алгебраическая система $\langle S, +, \cdot, 0, 1\rangle$, где $\langle S, +, 0\rangle$ — коммутативный моноид с нейтральным элементом нуль 0, $\langle S, \cdot, 1\rangle$ — моноид с нейтральным элементом единица 1, умножение дистрибутивно относительно сложения с обеих сторон и $0 \cdot a = a \cdot 0 = 0$ для всех $a \in S$. Коммутативное полукольцо, отличное от кольца, каждый ненулевой элемент которого обратим, называется *полуполем с нулем*.

Легко показать, что если S — полуполе с нулем, то $ab, a + b \neq 0$ для любых $a, b \in S\backslash\{0\}$. Поэтому множество $S\backslash\{0\}$ с теми же операциями сложения и умножения образует алгебраическую систему, которую будем называть *полуполем*.

Пусть S — это поле $\mathbb{R}$ действительных чисел, полуполе с нулем $\mathbb{R}_+$ неотрицательных действительных чисел или полуполе $\mathbb{P}$ положительных действительных чисел, рассматриваемых с интервальной топологией. Обозначим через $C(X, S)$ множество всех непрерывных S-значных функций, заданных на произвольном топологическом пространстве X, с поточечными операциями сложения и умножения. Тогда $C(X) = C(X, \mathbb{R})$ — кольцо, $C^+(X) = C(X, \mathbb{R}_+)$ — полукольцо и $U(X) = C(X, \mathbb{P})$ — полуполе.

Кольцо $C(X)$ является алгеброй над $\mathbb{R}$. Подалгеброй в $C(X)$ будет любое его подмножество, замкнутое относительно сложения и умножения функций и выдерживающее умножение на константы из $\mathbb{R}$. По аналогии назовем подмножество $A \subseteq C(X, S)$ *подалгеброй*, если $f + g, fg, rf \in A$ для любых $f, g \in A$ и $r \in S$. Таким образом, мы будем употреблять термин «подалгебра» в более широком смысле, нежели кольцо, одновременно являющееся векторным пространством.

Обозначим через $\mathbb{A}(C(X, S))$ *решетку всех подалгебр* в $C(X, S)$ относительно включения $\subseteq$ (строгое включение будем обозначать символом $\subset$), а через через $\mathbb{A}_1(C(X, S))$ — *решетку всех подалгебр с* 1.

Если A и B — подалгебры в $C(X, S)$, то точная нижняя грань $A \wedge B$ равна $A \cap B$, а точная верхняя грань $A \vee B$ состоит из конечных сумм функций вида $f_1 \cdot \ldots \cdot f_n$, где $f_1, \ldots, f_n \in A \cup B$, $n \in \mathbb{N}$. Если $S = \mathbb{R}$ или $S = \mathbb{R}_+$, то $A \cap B \neq \emptyset$, так как $0 \in A \cap B$. Напротив, если $S = \mathbb{P}$, то, возможно, $A \cap B = \emptyset$. Поэтому будем считать пустое множество $\emptyset$ элементом решетки $\mathbb{A}(U(X))$ — ее нулем.

Для любых $a, b \in \mathbb{R}$ положим $a \vee b = \max\{a, b\}$ и $a \wedge b = \min\{a, b\}$. Если в $\mathbb{P}$ заменить обычное сложение на max-сложение, то получим полуполе $\mathbb{P}^\vee$. Для полуполя $U^\vee(X) = C(X, \mathbb{P}^\vee)$ понятия подалгебры и решетки подалгебр (с единицей) определяются так же, как и в случае обычного сложения.

Подалгебру A назовем b-*подалгеброй*, если все функции из A ограничены сверху, sp-*подалгеброй*, если любая функция $f \in A$ строго положительна, т. е. $\inf f > 0$, и spb-*подалгеброй*, если она является b- и sp-подалгеброй одновременно.

Min_x — подалгебра функций, принимающих в точке x наименьшее значение.

Топологическое пространство X называется *хьюиттовским*, если оно гомеоморфно замкнутому подпространству некоторой тихоновской степени пространства $\mathbb{R}$. Хьюиттовскими пространствами являются, например, компакты, т. е. компактные хаусдорфовые пространства.

Напомним, что центральным результатом работы [1] является теорема 2, согласно которой топология любого хьюиттовского пространства X определяется решеткой $\mathbb{A}_1(U^\vee(X))$ и, как следствие (см. замечание после теоремы 2), решеткой $\mathbb{A}(U^\vee(X))$. Другими словами, для любых хьюиттовских пространств X и Y изоморфизм решеток $\mathbb{A}(U^\vee(X))$ и $\mathbb{A}(U^\vee(Y))$ или их подрешеток $\mathbb{A}_1(U^\vee(X))$ и $\mathbb{A}_1(U^\vee(Y))$ влечет гомеоморфизм пространств X и Y.

Возникают следующие естественные вопросы.

Вопрос 1. Как устроены изоморфизмы решеток $\mathbb{A}(U^\vee(X))$ и $\mathbb{A}(U^\vee(Y))$ и их подрешеток $\mathbb{A}_1(U^\vee(X))$ и $\mathbb{A}_1(U^\vee(Y))$?

Вопрос 2. Как устроены изоморфизмы полуполей $U^\vee(X)$ и $U^\vee(Y)$, которые порождают изоморфизмы решеток их подалгебр (с единицей)?

Вопрос 3. Существуют ли изоморфизмы решеток подалгебр (с единицей) полуполей $U^\vee(X)$ и $U^\vee(Y)$, которые не порождаются изоморфизмами самих полуполей?

Главная цель данной работы — ответить на вопросы 1–3.

Сделаем ряд предварительных замечаний.

1) Пусть α — изоморфизм решеток $\mathbb{A}_1(U^\vee(X))$ и $\mathbb{A}_1(U^\vee(Y))$, а α_X — канонический изоморфизм решеток $\mathbb{A}_1(spbU^\vee(X))$ и $\mathbb{A}_1(U^\vee(\beta X))$, где X и Y — хьюиттовские пространства, а βX — стоун-чеховская компактификация пространства X. При доказательстве [1, теорема 2] было показано, что соответствие $\varphi\colon \beta X \to \beta Y$, заданное правилом

$$\varphi(x) = y \Longleftrightarrow \alpha(\mathrm{Min}_x) = \mathrm{Min}_y,\ x \in \beta X, y \in \beta Y,$$

является гомеоморфизмом пространств βX и βY, причем ограничение $\varphi\big|_X$ служит гомеоморфизмом пространств X и Y. Отождествим точки пространств βX и βY гомеоморфизмом φ. Тогда можно считать, что изоморфизм α является автоморфизмом решетки $\mathbb{A}_1(U^\vee(X))$, который оставляет на месте подалгебры $\mathrm{spbMin}_x, x \in X$.

2) Пусть ψ — изоморфизм полуполей $U^\vee(X)$ и $U^\vee(Y)$, где X и Y — хьюиттовские пространства, который порождает изоморфизм решеток подалгебр $\mathbb{A}(U^\vee(X))$ и $\mathbb{A}(U^\vee(Y))$, а значит, и их подрешеток $\mathbb{A}_1(U^\vee(X))$ и $\mathbb{A}_1(U^\vee(Y))$. Тогда в силу замечания 1) точки пространств X и Y можно отождествить и считать, что изоморфизм ψ является автоморфизмом полуполя $U^\vee(X)$, который оставляет на месте подалгебры $\mathrm{spbMin}_x, x \in X$. В частности, $\psi(\mathbb{P}^\vee) = \mathbb{P}^\vee$, так как $\mathbb{P}^\vee$ есть пересечение подалгебр $\mathrm{spbMin}_x, x \in X$.

Ответим на вопрос 3.

Теорема 1. *Справедливы следующие утверждения*:

1) *автоморфизм ψ полуполя $U^\vee(X)$ порождает автоморфизм решетки $\mathbb{A}(U^\vee(X))$ тогда и только тогда, когда $\psi(\mathbb{P}^\vee) = \mathbb{P}^\vee$;*

2) *существуют автоморфизмы полуполей $U^\vee(X)$, которые не порождают автоморфизмы решеток $\mathbb{A}(U^\vee(X))$.*

Для любого числа $t > 0$ правило $f \mapsto f^t$ задает автоморфизм полуполя $U^\vee(X)$, который обозначим через ψ_t. Поскольку $\psi_t(\mathbb{P}^\vee) = \mathbb{P}^\vee$, по теореме 1 автоморфизм ψ_t порождает автоморфизм решетки $\mathbb{A}(U^\vee(X))$, который обозначим через α_t.

Ответим на вопрос 2.

Теорема 2. *Автоморфизмы ψ_t — это в точности все автоморфизмы полуполя $U^\vee(X)$, которые порождают автоморфизмы решетки $\mathbb{A}(U^\vee(X))$, оставляющие на месте подалгебры* spbMin_x, $x \in X$.

Если пространство X конечно, то функции полуполя $U^\vee(X)$ можно записывать в виде набора значений функции в точках X, предварительно зафиксировав порядок точек X. Например, если $X = \{x, y, z\}$ и функция $f \in U^\vee(X)$ такая, что $f(x) = 8$, $f(y) = 4$ и $f(z) = 2$, то $f = (8, 4, 2)$ или, что равносильно, $f = 8(1, 1/2, 1/4)$.

Пусть $X = \{x, y, z\}$. Обозначим через $U^\vee_y(X)$ множество функций

$$U^\vee_y(X) = \{f \in U^\vee(X) \colon \min f < f(y) < \max f\}.$$

Множества $U^\vee_x(X)$ и $U^\vee_z(X)$ определим аналогичным образом.

Зафиксируем пару чисел a_y и s_y, где $s_y > 1 > a_y > 0$. Тогда для любой функции $f \in U^\vee_y(X)$ найдутся числа $r, p > 0$ и k такие, что

$$f = \begin{cases} a_y^k\left(1, a_y^r, (a_y^r)^{1+p(s_y-1)}\right), \text{ если } f(x) > f(y) > f(z), \\ a_y^k\left((a_y^r)^{1+p(s_y-1)}, a_y^r, 1\right), \text{ если } f(x) < f(y) < f(z). \end{cases}$$

Зафиксируем еще одну пару чисел a и s, где $s > 1 > a > 0$. Легко видеть, что правило

$$a^k\left(1, a^r, (a^r)^{1+p(s-1)}\right) \mapsto a_y^k\left(1, a_y^r, (a_y^r)^{1+p(s_y-1)}\right),$$
$$a^k\left((a^r)^{1+p(s-1)}, a^r, 1\right) \mapsto a_y^k\left((a_y^r)^{1+p(s_y-1)}, a_y^r, 1\right),$$

задает преобразование множества $U^\vee_y(X)$, которое обозначим через ψ_{T_y}, где $T_y = (a, a_y; s, s_y)$ — набор параметров, задающих ψ_{T_y}. Аналогичным образом определим преобразования ψ_{T_x} и ψ_{T_z}, где $T_x = (a, a_x; s, s_x)$ и $T_z = (a, a_z; s, s_z)$.

Обозначим через T набор параметров $T = (a, a_x, a_y, a_z; s, s_x, s_y, s_z)$, который задает набор преобразований ψ_{T_x}, ψ_{T_y} и ψ_{T_z}. Тогда соответствие $\psi_T \colon U^\vee(X) \to U^\vee(X)$, заданное правилом

$$\psi_T(f) = \begin{cases} \psi_{T_x}(f), \text{ если } f \in U^\vee_x(X), \\ \psi_{T_y}(f), \text{ если } f \in U^\vee_y(X), \\ \psi_{T_z}(f), \text{ если } f \in U^\vee_z(X), \\ f, \text{ если } |\operatorname{Im} f| \le 2, \end{cases}$$

будет преобразованием полуполя $U^{\vee}(X)$, которое совпадает с некоторым автоморфизмом ψ_t полуполя $U^{\vee}(X)$ тогда и только тогда, когда $a_x = a_y = a_z$ и $s_x = s_y = s_z = s$.

Предложение 1. *Пусть $X = \{x, y, z\}$. Тогда любое преобразование ψ_T полуполя $U^{\vee}(X)$ порождает автоморфизм решетки $\mathbb{A}_1(U^{\vee}(X)$, который оставляет на месте подалгебры* $\mathrm{spbMin_x}, \mathrm{spbMin_y}$ *и* $\mathrm{spbMin_z}$.

Обозначим через α_T автоморфизм решетки $\mathbb{A}_1(U^{\vee}(X)$, который порождается преобразованием ψ_T.

Следующая теорема отвечает на вопрос 1 в части решеток подалгебр $\mathbb{A}_1(U^{\vee}(X))$.

Теорема 3. *Автоморфизмы решетки $\mathbb{A}_1(U^{\vee}(X))$, которые оставляют на месте подалгебры* $\mathrm{spbMin_x}$, $x \in X$, *— это в точности ограничения автоморфизмов α_t на решетку $\mathbb{A}_1(U^{\vee}(X))$ в случае $|X| \neq 3$ и автоморфизмы α_T в случае $|X| = 3$.*

Пусть $X = \{x, y\}$. Зафиксируем пару автоморфизмов w_x и w_y цепи $(0, 1]$. Тогда соответствие $\psi_{w_x, w_y}\colon U^{\vee}(X) \to U^{\vee}(X)$, заданное правилом

$$\psi_{w_x,w_y}(f) = \begin{cases} f(y)\left(w_x\left(\dfrac{f(x)}{f(y)}\right), 1\right), \text{ если } f(x) > f(y), \\ f(x)\left(1, w_y\left(\dfrac{f(y)}{f(x)}\right)\right), \text{ если } f(x) < f(y), \\ f, \text{ если } f(x) = f(y), \end{cases}$$

будет преобразованием полуполя $U^{\vee}(X)$.

Предложение 2. *Пусть $X = \{x, y\}$. Тогда любое преобразование ψ_{w_x,w_y} полуполя $U^{\vee}(X)$ порождает автоморфизм решетки $\mathbb{A}(U^{\vee}(X)$, который оставляет на месте подалгебры* $\mathrm{spbMin_x}$ *и* $\mathrm{spbMin_y}$.

Обозначим через α_{w_x,w_y} автоморфизм решетки $\mathbb{A}(U^{\vee}(X)$, который порождается преобразованием ψ_{w_x,w_y}.

Наконец, ответим на вопрос 1 в части решеток подалгебр $\mathbb{A}(U^{\vee}(X)$.

Теорема 4. *Автоморфизмы решетки $\mathbb{A}(U^{\vee}(X))$, которые оставляют на месте подалгебры* $\mathrm{spbMin_x}$, $x \in X$, *— это в точности автоморфизмы α_t в случае $|X| \neq 2$ и автоморфизмы α_{w_x,w_y} в случае $|X| = 2$.*

Работа выполнена при финансовой поддержке Минобрнауки РФ (проект №1.5879.2017/8.9).

Литература

1. Sidorov V.V., *Determinability of Hewitt spaces by the lattices of subalgebras with unit of semifields of continuous positive functions with max-plus* // Lobachevskii J. Math. – 2017. – V. 38. – № 4. – P. 741–750.

ISOMORPHISMS OF LATTICES OF SUBALGEBRAS OF SEMIFIELDS OF CONTINUOUS POSITIVE FUNCTIONS WITH MAX-PLUS

V.V. Sidorov

Isomorphisms of lattices of subalgebras of semifields of continuous positive functions are characterized.

Keywords: semifield of continuous functions, lattice of subalgebras, isomorphism, Hewitt space.

УДК 519.7; 512.581

ОБ ОДНОЙ СХЕМЕ ЦИФРОВОЙ ПОДПИСИ НА ПЛАТФОРМЕ 2-КАТЕГОРИЙ

О.П. Соболев[1]

1 *o.sobolev94@yandex.ru*; Казанский (Приволжский) федеральный университет

В данной статье рассмотрена модификация цифровой подписи. Модификация осуществлена путем использования в качестве криптографической платформы 2-категории.

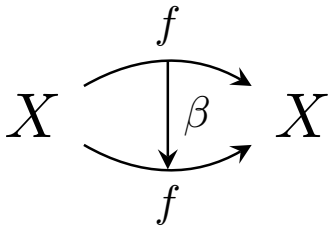
Ключевые слова: цифровая подпись, 2-категории, алгебраическая криптография.

В данной работе показывается, как можно осуществить один протокол цифровой подписи (аналог подписи из [1]) с использованием алгебраической платформы 2-категорий. Подробные описания 2-категорий можно найти в [2], [3] и [4]. Насколько нам известно, прежде 2-категории в криптографии не использовались. Протокол из [1] нетрудно переписать для случая обычных категорий. Приведем реализацию аналогичной идеи в случае, когда алгебраической платформой будут 2-категории. Это означает, что имеются не только обычные морфизмы (1-морфизмы), но и морфизмы между морфизмами (2-морфизмы), обладающие рядом свойств, которые можно найти в указанной выше литературе.

Вначале опишем используемые обозначения, H – открытая хеш-функция, k – фиксированное число $H : \{0,1\}^* \to \{0,1\}^k$, $k \in \mathbb{Z}$, $e \in \mathbb{Z}$ – открытый ключ, m – сообщение для подписи, в виде битовой строки.

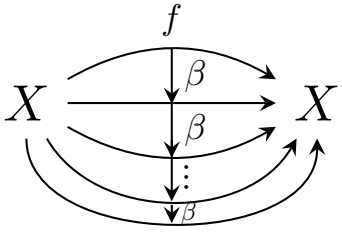
Секретный ключ состоит из двух частей:

1) 2-морфизм $\beta : f \to f$, т. е.

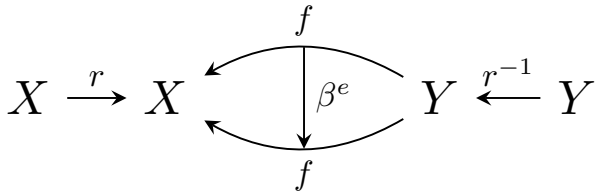


2) Обратимый 1-морфизм $r : X \to Y$

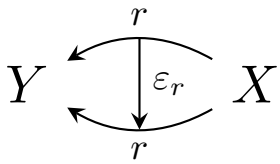
Это дает возможность образовать 2-морфизм $\alpha = r\, b^e\, r^{-1}$, где b^e – вертикальная суперпозиция:



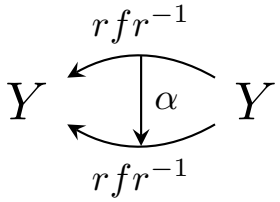
горизонтальная суперпозиция:



$r\beta^e r^{-1} = \varepsilon_r \circ \beta^e \circ \varepsilon_{(r^{-1})}$, где ε_r – единица относительно вертикальной суперпозиции:



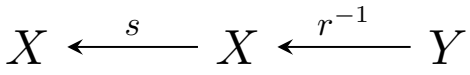
Так что α есть:



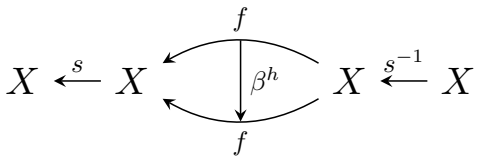
1-стрелка rfr^{-1} известна, но r и f - части секретного ключа.

Протокол подписи.

1. Вычисляется $h = H(m)$.
2. Выбирается случайным образом обратимый 1-морфизм $s : X \to X$
3. Вычисляется $t = sr^{-1}$ – 1-морфизм, первая часть подписи:



4. $v = s\beta^h s^{-1}$ – вторая часть подписи. Это 2-морфизм:



5. Подпись – (t, v).

Проверка подписи.
Проверяющий знает e, α, m, t, v.

1. Вычисляется $h = H(m)$.
2. $\gamma = \alpha^h = r\beta^{eh}r^{-1}$

3. Проверочные соотношения: $v^e = t\gamma t^{-1}$?= $s\beta^{eh}s^{-1}$. Учитывая, что $t = sr^{-1}$:

$$t\gamma t^{-1} = sr^{-1}(r\beta^{eh}r^{-1})rs^{-1} = s\beta^{eh}s^{-1}.$$

Отметим, что возможен аналог этого протокола, использующий только горизонтальную суперпозицию в 2-категориях.

Литература

1. Baocang Wang, Yupu Hu *Signature scheme using the root extraction problem on quaternions* // Journal of Applied Mathematics. – V. 2014. – Article ID 819182. – 7 p.

2. Power J. *2-Categories*. – BRICS Notes Series. –1998. – V. NS98-7. – 28 p.

3. Маклейн С. *Категории для работающего математика*. – М.: Физматлит, 2004. – 352 с.

4. Gray J. W. *Formal Category Theory: Adjointness for 2-Categories*. – Springer, 1974. (Lecture Notes in Mathematics 391). – XII+282 p.

ABOUT ONE SCHEME OF DIGITAL SIGNATURES ON A 2-CATEGORY PLATFORM

O.P. Sobolev

In this paper, a modification of the digital signature is considered. The modification was implemented by using the 2-category as a cryptographic platform.

Keywords: digital signature, 2-category, algebraic cryptography.

УДК 517.956.3

К НОВЫМ СЛУЧАЯМ РАЗРЕШИМОСТИ ЗАДАЧИ ГУРСА В КВАДРАТУРАХ ДЛЯ СИСТЕМЫ ВТОРОГО ПОРЯДКА

Е.А. Созонтова[1]

1 *sozontova-elena@rambler.ru*; Елабужский институт КФУ

В статье описываются новые варианты разрешимости задачи Гурса в квадратурах для двумерной системы второго порядка.

Ключевые слова: задача Гурса, разрешимость в квадратурах.

Задача 1. В области D найти регулярное решение системы

$$\begin{cases} u_{xy} + a_1 u_x + b_1 u_y + c_1 v_x + d_1 v_y + e_1 u + f_1 v = g_1, \\ v_{xy} + a_2 u_x + b_2 u_y + c_2 v_x + d_2 v_y + e_2 u + f_2 v = g_2, \end{cases} \tag{1}$$

удовлетворяющее условиям

$$\begin{gathered} u(x_0, y) = \varphi_1(y),\ u(x, y_0) = \psi_1(x),\ v(x_0, y) = \varphi_2(y),\ v(x, y_0) = \psi_2(x), \\ \varphi_1(y_0) = \psi_1(x_0), \quad \varphi_2(y_0) = \psi_2(x_0). \end{gathered} \tag{2}$$

При этом, предполагается, что $\varphi_1,\ \varphi_2 \in C^1(\overline{X}),\ \psi_1,\ \psi_2 \in C^1(\overline{Y})$, а гладкость коэффициентов системы (1) определяется включениями

$$a_1,\ a_2,\ c_1,\ c_2 \in C^{(1,0)},\ b_1,\ c_1,\ c_2,\ d_2 \in C^{(0,1)},\ e_1,\ e_2,\ f_1,\ f_2 \in C^{(0,0)}.$$

Известно [1, с. 67], что решение этой задачи существует и единственно. В [2] получены условия разрешимости задачи 1 в квадратурах. В настоящей работе приводятся новые случаи разрешимости указанной задачи в явном виде. Важную роль при этом играют играют следующие соотношения и тождества

$$\begin{gathered} h = a_x + ab - c,\ k = b_y + ab - c, \\ \omega_r = \frac{2s_r'(x)t_r'(y)}{(2-m_r)[s_r(x)+t_r(y)]^2},\ [s_r(x) + t_r(y)]s_r'(x)t_r'(y) \neq 0. \end{gathered} \tag{3}$$

$$\begin{gathered} 1)\ h \equiv 0;\ 2)\ k \equiv 0;\ 3)\ 2h - (\ln h)_{xy} - k \equiv 0;\ 4)\ 2k - (\ln k)_{xy} - h \equiv 0; \\ 5)\ a_x \equiv b_y,\ h \equiv \xi_0(x)\eta_0(y) \neq 0;\ 6)\ b_y - a_x \equiv h \equiv \xi_1(x)\eta_1(y) \neq 0; \\ 7)\ a_x - b_y \equiv k \equiv \xi_2(x)\eta_2(y) \neq 0;\ 8)\ h \equiv 2\mu_0(x)\tau_0(y) \neq 0,\ k \equiv 3\mu_0(x)\tau_0(y) \neq 0; \\ 9)\ h \equiv 3\mu_1(x)\tau_1(y) \neq 0,\ k \equiv 2\mu_1(x)\tau_1(y) \neq 0;\ 10)\ (\ln h)_{xy} \equiv h - k,\ h \equiv 2b_y \equiv \omega_1; \\ 11)\ (\ln k)_{xy} \equiv k - h,\ k \equiv 2a_x \equiv \omega_2;\ 12)\ m_0 a_x - b_y \equiv m_0 b_y - a_x \equiv (m_0 - 1)(ab - c); \\ 13)\ h \equiv \omega_0;\ 14)\ k \equiv \omega_0. \end{gathered} \tag{4}$$

$$c_1 \equiv d_1 \equiv f_1 \equiv 0. \tag{5}$$

$$a_2 \equiv b_2 \equiv f_2 \equiv 0. \tag{6}$$

$$a = a_1,\ b = b_1,\ c = e_1. \tag{7}$$

$$a = c_2,\ b = d_2,\ c = f_2. \tag{8}$$

Справедлива теорема

Теорема 1. *Для разрешимости задачи 1 в квадратурах достаточно, чтобы выполнялся один из наборов тождеств тождества (5), (6) и каждый из двух наборов a, b, c, определяемых формулами (7), (8), удовлетворял условиям: или выполняется одно из тождеств 1) – 4) в (4), или существуют функции ξ_r, η_r, μ_r, τ_r, m_r, s_r, t_r, для которых имеет место любая из групп соотношений 5) – 11), или когда вместе с 12) любая из определяемых в (3) комбинаций h, k имеет вид, указанный в 13) – 14), при этом зависящая лишь от одной из переменных (x, y) функция ω_0 удовлетворяет условию $\omega_0 \neq 0$, а ω_1, $\omega_2 - (\omega_k + 1)(\omega_k - 2) \neq 0$.*

Здесь $\xi_r,\ \eta_r \in C^1,\ s_r,\ t_r,\ m_0 \in C^2$, причем m зависит только от одной из переменных (x, y) и $m \neq 2$

Литература

1. Бицадзе А.В. *Некоторые классы уравнений в частных производных*. – М.: Наука, 1981. – 448 с.

2. Созонтова Е.А. *Об условиях разрешимости граничных задач в квадратурах для гиперболических систем второго порядка* // Уфимск. матем. журн. – 2016. – Т. 8, вып. 3. – С. 135–140.

NEW CASES OF SOLVABILITY OF THE GOURSAT PROBLEM IN QUADRATURES FOR THE SYSTEM OF SECOND ORDER

E.A. Sozontova

The article describes new cases of solvability of the Goursat problem in quadratures for two-dimensional system of second order.

Keywords: the Goursat problem, solvability in quadratures.

УДК 512.55

ГРУППА АВТОМОРФИЗМОВ КОЛЕЦ ФОРМАЛЬНЫХ МАТРИЦ

Д.Т. Тапкин[1]

1 *danil.tapkin@yandex.ru*; Казанский (Приволжский) федеральный университет

Были разобрана проблема изоморфизма для колец верхнетреугольных формальных матриц и колец формальных матриц с нулевыми идеалами следа. Получен явный вид изоморфизма. Для специального класса колец формальных матриц показано, что все R-автоморфизмы являются внутренними.

Ключевые слова: кольца формальных матриц, нулевые идеалы следа, изоморфизм, автоморфизм, внутренний автоморфизм.

В последнее десятилетие широкое распространение получило исследование колец формальных матриц (см. [1-4], [6-8], [13], [14]). Многие из результатов, полученных в последнее время, нашли отражение в монографии [5]. Впервые вопрос изоморфизма колец верхнетреугольных формальных матриц был изучен в [12]. Позднее в [9] этот результат был усилен, и был получен явный вид изоморфизма для колец верхнетреугольных формальных матриц порядка 2. В [10] было получено необходимое и достаточное условие для существования изоморфизма между двумя кольцами верхнетреугольных формальных матриц порядка n. И, наконец, в [11] был получен явный вид изоморфизма для колец формальных матриц второго порядка с нулевыми идеалами следа.

При изучении проблемы изоморфизма удалось получить явный вид изоморфизма для следующих классов колец формальных матриц порядка n: кольца верхнтреугольных формальных матриц и кольца формальных матриц с нулевыми идеалами следа. При определенных ограничениях на диагональные кольца, в обоих случах изоморфизм является поэлементным, с точностью до перестановки и сопряжения.

Полученные результаты позволили установить следующий факт. Пусть R – коммутативное кольцо. Через $Q(R)$ будем обозначать полное кольцо частных $S^{-1}R$, где S – множество неделителей нуля кольца R.

Теорема 1. *Пусть R – коммутативное кольцо без нетривиальных идемпотентов, $n \in \mathbb{N}$ и $\{I_{ij}\}_{1\leq i<j\leq n}$ – набор идеалов кольца R, каждый из которых содержит хотя бы один элемент неделитель нуля, при этом потребуем, чтобы выполнялось $I_{ij}I_{jk} \subseteq I_{ik}$ для каждой тройки $i < j < k$. Пусть также $A = T_n((R);\{I_{ij}\}) \subseteq T_n(Q(R))$ – кольцо формальных матриц с естественными операциями матричного сложения и умножения. Тогда все R-автоморфизмы кольца A представимы в виде композиции $C_U \circ C_V$, где $U \in U(A)$, $V = \mathrm{diag}(h_1, ..., h_n) \in U(T_n(Q(R)))$, $C_V(A) = A$.*

Существуют примеры, показывающие что в общем случае избавиться от автоморфизма C_V не удается. Однако, верен следующий результат.

Теорема 2. *Пусть в условии теоремы 1 целое замыкание кольца R в $Q(R)$ совпадает с R и идеалы I_{ij} конечно порождены. Тогда все R-автоморфизмы кольца A внутренние.*

Хорошо известными примерами целозамкнутых колец являются дедекиндовы кольца и факториальные кольца. Более того, в силу нетеровости дедекиндовых колец, все их идеалы конечно порождены.

Следствие 1. *Пусть R – дедекиндово кольцо, $n \in \mathbb{N}$ и $\{I_{ij} \mid 1 \le i < j \le n\}$ – набор ненулевых идеалов кольца R, таких что $I_{ij}I_{jk} \subseteq I_{ik}$ для каждой тройки $i < j < k$. Пусть также $A = T_n((R); \{I_{ij}\}) \subseteq T_n(Q(R))$ – кольцо формальных матриц с естественными операциями матричного сложения и умножения. Тогда все R-автоморфизмы кольца A являются внутренними.*

Теорема 3. *Пусть R – факториальное кольцо, $n \in \mathbb{N}$ и $\{I_{ij} \mid 1 \le i < j \le n\}$ – набор ненулевых идеалов кольца R, таких что $I_{ij}I_{jk} \subseteq I_{ik}$ для каждой тройки $i < j < k$. Пусть также $A = T_n((R); \{I_{ij}\}) \subseteq T_n(Q(R))$ – кольцо формальных матриц с естественными операциями матричного сложения и умножения. Тогда все R-автоморфизмы кольца A являются внутренними.*

Литература

1. Абызов А. Н., Тапкин Д. Т. *Кольца формальных матриц и их изоморфизмы* // Сиб. мат. журнал. – 2015. – Т. 56. – С. 1199–1214.

2. Абызов А. Н., Тапкин Д. Т. *О некоторых классах колец формальных матриц* // Изв. вузов. Матем. – 2016. –№ 3. – С. 3–14.

3. Крылов П. А. *Об изоморфизме колец обобщенных матриц* // Алгебра и логика. –2008. – Т. 47 – № 4. – С. 456–463.

4. Крылов П. А., Туганбаев А. А. *Формальные матрицы и их определители* // Фундамент. и прикл. матем. – 2014. – Т. 19. – № 1. – С. 65–119.

5. Крылов П. А., Туганбаев А. А. *Кольца формальных матриц и модули над ними*. – М.: МЦНМО, 2017. – 192 с.

6. Тапкин Д. Т. *Кольца формальных матриц и обобщение алгебры инцидентности* // Чебышевский сб. – 2015. – Т. 16. – № 3 – С. 422–449.

7. Тапкин Д. Т. *Изоморфизмы колец инцидентности формальных матриц* // Изв. вузов. Матем. – 2017. – № 12.

8. Тапкин Д. Т. *Изоморфизмы колец формальных матриц с нулевыми идеалами следа* // Сиб. мат. журнал – принята в печать.

9. Anh P. N., van Wyk L. *Automorphism group of generalized triangular matrix rings* // Linear Algebra and its Appl. – 2011. – V. 434. – P. 1018–1026.

10. Anh P. N., van Wyk L., *Isomorphisms between strongly triangular matrix rings* // Linear Algebra and its Appl. – 2013. – V. 438. – P. 4374–4381.

11. Boboc C., Dascalescu S., van Wyk L., *Isomorphisms between Morita context rings* // Linear and Multilinear Algebra. – 2012. – V. 60. – P. 545–563.

12. Khazal R., Dascalescu S., van Wyk L. *Isomorphisms of generalized triangular matrix-rings and recovery of tiles* // Internat. J. Math. Math. Sci. – 2003. – V. 2003. – № 9. – P.533–538.

13. Tang G., Zhou Y. *A class of formal matrix ring* // Linear Algebra and its Appl. – 2013. – V. 438. – № 12. – P. 4672–4688.

14. Tang G., Li C., Zhou Y. *Study of Morita contexts* // Comm. in Algebra. – 2014. – V. 42. – № 4. – P. 1668–1681.

AUTOMORPISM GROUP OF FORMAL MATRIX RINGS

D.T. Tapkin

Isomorphism problem was studied for upper-triangular formal matrix rings and for formal matrix rings with zero trace ideals. Explicit isomorphism criteria was found. For special case of formal matrix rings it was shown that all R-automorphisms are inner.

Keywords: formal matrix rings, zero trace ideals, isomorphism, automorphism, inner automorphism.

УДК 517.956.25

МАССИВНЫЕ МНОЖЕСТВА И ТЕОРЕМЫ ТИПА ЛИУВИЛЛЯ

В.В. Филатов[1]

1 *vladimfilatov@yandex.ru*; Волгоградский государственный университет, Институт математики и информационных технологий

В статье рассматриваются решения одного полулинейного уравнения на произвольных некомпактных римановых многообразиях с пустым краем. Доказана взаимосвязь между существованием нетривиальных ограниченных решений и существованием L-массивных множеств.

Ключевые слова: массивные множества, теоремы типа Лиувилля, эллиптические уравнения, римановы многообразия.

Данная работа посвящена изучению взаимосвязи между существованием нетривиальных ограниченных решений уравнения

$$Lu = \Delta u - u\phi(|u|) = 0, \tag{1}$$

и существованием L-массивных подмножеств, на произвольном некомпактном римановом многообразии M. Здесь $\phi(\xi)$ – неотрицательная, монотонно неубывающая непрерывно дифференцируемая функция при $\xi \geq 0$.

Данная тематика имеет прямое отношение к теоремам типа Лиувилля. Считающаяся в настоящее время классической формулировка теоремы Лиувилля утверждает, что всякая ограниченная гармоническая функция в $\mathbb{R}^n$ есть тождественная постоянная. Традиционно осуществляется следующий подход к теоремам типа Лиувилля. Пусть на римановом многообразии M задан класс функций A и эллиптический оператор L. Говорят, что на M выполнено (A, L) лиувиллево свойство, если любое решение уравнения $Lu = 0$, принадлежащее функциональному классу A, является тождественной постоянной.

В последние несколько десятилетий был опубликован ряд работ, посвященных выполнению теорем типа Лиувилля на произвольных некомпактных римановых многообразиях. Приводятся условия на геометрию римановых многообразий в терминах роста объема, условий на кривизну, выполнения изопериметрических неравенств и так далее.

В качестве примера можно привести один из первых геометрических результатов в классификационной теории римановых многообразий, а именно известную

теорему из [1]. Последняя утверждает, что если на многообразии объем геодезического шара радиуса R растет не быстрее R^2 при $R \to \infty$, то многообразие имеет параболический тип, то есть на нем любая положительная супергармоническая функция является тождественной постоянной.

В [2] было доказано, что на многообразии существует нетривиальная ограниченная гармоническая функция тогда и только тогда, когда существует гладкая гиперповерхность разделяющая многообразие на два массивных подмножества.

В ряде работ рассматривались аналогичные задачи для решений эллиптических уравнений более общих, чем уравнение Лапласса-Бельтрами, например, стационарное уравнению Шрёдингера $\Delta u - q(x)u = 0$. Однако в случае стационарного уравнения Шрёдингера ненулевая постоянная не будет являться его решением, поэтому и теоремы типа Лиувилля формулируется несколько иначе. В качестве иллюстрации можно привести следующие работы [5], [6].

В [3] была получена взаимосвязь между размерностью пространств решений стационарного уравнения Шрёдингера и существованием q массивных подмножеств. Ряд работ был посвящён исследованию решений полулинейного уравнения (1), например, [4], [7].

Данная работа, в некотором смысле обобщает результат, полученный в [3], на случай полулинейного уравнения. Однако в работе [3] были получены оценки размерностей пространств решений, что в данном случае не представляется возможным.

Перейдём к точным формулировкам. Пусть M – некомпактное риманово многообразие с пустым краем.

Непрерывную функцию u, определённую на открытом множестве $\Omega \subset M$, будем называть субрешением (суперрешением) уравнения (1), если для любой области $G \subset\subset \Omega$ и для любого v – решения (1), удовлетворяющего условиям

$$v \in C(\overline{G}),\ u|_{\partial G} = v|_{\partial G},$$

выполнено $u \le v$ ($u \ge v$) в G.

Открытое собственное подмножество $\Omega \subset M$ будем называть L-массивным, если на M существует нетривиальное субрешение уравнения (1) такое, что

$$\begin{cases} u = 0, x \in M \setminus \Omega, \\ 0 \le u \le 1. \end{cases}$$

Такую функцию будем называть внутренним потенциалом множества Ω. Отметим, что понятие массивного множества было введено в [2] для гармонических функций, а позже было обобщено в [3] для решений стационарного уравнения Шрёдингера.

Очевидно, что L-массивное множество не компактно. Действительно, пусть Ω – компактное L-массивное множество, но тогда для любого решения, такого что $u|_{\partial\Omega} = 0$ в силу принципа максимума выполнено $u = 0$ на Ω, а из определения субрешений следует их тривиальность.

Теорема. *На многообразии M существует нетривиальное ограниченное решение уравнения* (1) *тогда и только тогда, когда существует L-массивное подмножество M*

Лемма 1. *Пусть $B \subset M$ – предкомпактное, открытое подмножество M с гладкой*

границей. Если для функции и выполнено $Lu \geq 0 (Lu \leq 0)$ *в* B*, то*

$$\sup_B u \leq \sup_{\partial B} u^+ \quad (\inf_B u \geq \inf_{\partial B} u^-).$$

Лемма 2. *Пусть* $B \subset M$ *– произвольное предкомпактное открытое подмножество.* $\{u_i\}_{i=1}^{\infty}$ *– равномерно ограниченное на* B *семейство решений уравнения* (1)*,* $u_i \in C^{2,\alpha}(B)$*. Тогда семейство функций* $\{u_i\}_{i=1}^{\infty}$ *компактно в классе* $C^2(B')$*.*

Лемма 3. *Пусть* $B \subset M$ *– предкомпактное, открытое подмножество* M *с гладкой границей. Если для функций* $u, v \in C^2(B) \cap C^0(\partial B)$ *выполнено* $Lu \geq Lv$ *в* B *и* $u \leq v$ *на* ∂B*, то* $u \leq v$ *в* B*.*

Работа выполнена при финансовой поддержке РФФИ (проект 15-41-02479 р_поволжье_а).

Литература

1. Cheng S.Y., Yau S.T. *Differential equations on Riemannian manifolds and their geometric applications* // Comm. Pure and Appl. Math. – 1975. – V. 28. – № 3. – P. 333–354.

2. Григорьян А.А., *О лиувиллевых теоремах для гармонических функций с конечным интегралом Дирихле* // Матем. сб. – 1987. – Т. 132(174), вып. 4. – С. 496–516.

3. Григорьян А.А., Лосев А.Г. *О размерности пространств решений стационарного уравнения шредингера на некомпактных римановых многообразиях* // Матем. физика и комп. моделир. – 2017. – Т. 20, вып. 3. – С. 34–42.

4. Ландис Е.М. *Уравнения второго порядка эллиптического и параболического типов*. – М.: Наука, 1971. – 288 с.

5. Лосев А.Г., Мазепа Е.А. *Ограниченные решения уравнения Шрёдингера на римановых произведениях* // Алгебра и анализ. – 2001. – Т. 13, № 1. – С. 84–110;

6. Лосев А.Г., Мазепа Е.А., Чебаненко В.Ю. *О неограниченных решениях стационарного уравнения Шрёдингера на модельных римановых многообразиях* // Изв. вузов. Матем. – 2006. – № 7. – С. 46–56.

7. Мазепа Е.А. *Краевые задачи и лиувиллевы теоремы для полулинейных эллиптических уравнений на римановых многообразиях* // Изв. вузов. Матем. – 2005. – № 3. – С. 59–66.

MASSIVE SETS AND LIOUVILLE TYPE THEOREMS

V.V. Filatov

We study some property of half-linear equation on non-compact Riemannian manifolds. We establish connection between existing of nontrivial bounded solution and existing L*-massive sets.*

Keywords: Riemannian manifolds, Liouville type theorems, massive sets, elliptic equations.

УДК 517.928

ИНВАРИАНТНАЯ ПОВЕРХНОСТЬ СО СМЕНОЙ УСТОЙЧИВОСТИ В МОДЕЛИРОВАНИИ КРИТИЧЕСКИХ ЯВЛЕНИЙ ЭЛЕКТРОКАТАЛИТИЧЕСКОЙ РЕАКЦИИ

Н.М. Фирстова[1]

1 *firstova.natalia@yandex.ru*; Самарский национальный исследовательский университет им. академика С.П. Королева

В работе на основе геометрического подхода и теории интегральных многообразий сингулярно возмущенных систем исследована модель электрокаталитической реакции, лежащей в основе действия электрохимических реакторов. Получена многомерная инвариантная поверхность со сменой устойчивости. Показано, что данная поверхность состоит из траекторий-уток, каждая из которых моделирует критический режим в рассматриваемой системе.

Ключевые слова: траектории-утки, критические явления, инвариантная поверхность со сменой устойчивости, сингулярные возмущения.

1. Динамическая модель электрокаталитической реакции

Рассматриваемая модель электрокаталитической реакции с учетом внешнего сопротивления цепи [1] имеет вид:

$$\begin{aligned} \epsilon\frac{dE}{d\tau} &= \frac{\nu-E}{r} - k_b\theta e^{-bE} = R(E,u,\theta), \\ \frac{du}{d\tau} &= -u(\theta_A-\theta)k'_a e^{-cE} + 1 - u = Q(E,u,\theta), \\ \frac{d\theta}{d\tau} &= u(\theta_A-\theta)\bar{k}_a e^{-cE} - k_b\theta e^{-bE} = H(E,u,\theta), \end{aligned} \tag{1}$$

где E — электродный потенциал, u — объемная концентрация электроактивного вещества у электрода, θ_A — поверхность, занятая адсорбированным катализатором, θ — поверхность, на которой катализатор связан комплексом с ионом восстанавливаемого компонента, r — сопротивление цепи, k_b — константа скорости катодной реакции, k_a — константа скорости комплексообразования, ν — контролируемый потенциал сети. Так как параметр ϵ мал, то система (1) является сингулярно возмущенной. Поставим перед собой задачу исследовать динамику поведения решений в зависимости от значений дополнительных параметров дифференциальной системы. Исследование проведем с помощью методов теории сингулярных возмущений и численными методами [2].

Уравнение медленной поверхности (нулевого приближения медленного инвариантного многообразия системы [2]) описывается вырожденным уравнением системы (1):

$$\frac{\nu-E}{r} - k_b\theta e^{-bE} = 0. \tag{2}$$

Как показано в [3], в рассматриваемой модели существует кривая срыва, разделяющая медленную поверхность на устойчивую и неустойчивую части, и система

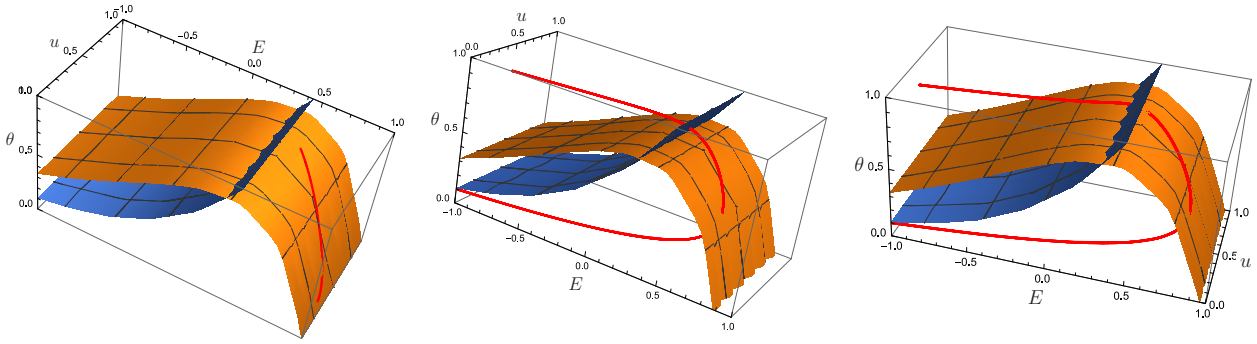
(1) имеет одно положение равновесия:

$$A\left(E^*, \frac{(v-E^*)e^{cE^*}}{r\bar{k}_a(\theta_A - e^{bE^*}\frac{v-E^*}{k_b r})}, \frac{v-E^*}{k_b r}e^{bE^*}\right),$$

где E^* — решение следующего уравнения:

$$-\frac{(v-E)}{k'_a}r\bar{k}_a + 1 - \frac{(v-E)e^{cE}}{\bar{k}_a(\theta_A - e^{bE}\frac{v-E}{k_b r})} = 0.$$

Положение особой точки на медленной поверхности и её тип зависят от соотношения параметров системы. При фиксации всех значений параметров, кроме одного, управляющего, было выделено три основных режима системы: безопасный режим (рис. 1а), режим с самоускорением (рис. 1б) и критический режим (рис. 1в), играющий роль водораздела между первыми двумя режимами. В [3] было показано, что критический режим отвечает случаю, когда особая точка находится на неустойчивой части медленной поверхности, но в малой, порядка $O(\epsilon)$, окрестности кривой срыва.



а) б) в)

Рис. 1. Режимы системы: а) безопасный режим, б) режим с самоускорением, в) критический режим.

Если выбором значения управляющего параметра можно «склеить» притягивающее и отталкивающее медленные инвариантные многообразия в точке срыва, то система (1) будет иметь решение-утку, отвечающее критическому режиму химической реакции, разграничивающему области медленных и быстрых режимов [4, 5].

Начальные условия для рассматриваемой системы не фиксированы, поэтому притягивающие и отталкивающие инвариантные многообразия целесообразно «склеить» не в одной точке кривой срыва, а во всех её точках одновременно, построив тем самым инвариантную поверхность со сменой устойчивости, целиком состоящую из траекторий-уток. Каждая из этих уток моделирует критические режимы, отвечающие конкретному начальному условию, и проходит через определенную точку на кривой срыва.

2. Инвариантная поверхность со сменой устойчивости

Для того чтобы упростить расчеты и получить в системе (1) единый параметр k_a, преобразуем её следующим образом:

$$\begin{aligned} \epsilon\frac{dE}{d\tau} &= \frac{\nu-E}{r} - k_b\theta e^{-bE} = R(E,u,\theta), \\ \frac{du}{d\tau} &= -u(\theta_A-\theta)k_a e^{-cE} + 1 - u = Q(E,u,\theta), \\ \beta\frac{d\theta}{d\tau} &= u(\theta_A-\theta)k_a e^{-cE} - k_b\theta e^{-bE} = R(E,u,\theta), \end{aligned} \tag{3}$$

где β — безразмерная объемная концентрация вещества.

В качестве склеивающей функции инвариантного многообразия со сменой учтойчивости $\theta = \theta(u,E,\epsilon)$ рассмотрим $k_a = k_a(u,\epsilon)$, где:

$$\begin{aligned} \theta &= \theta_0(u,E) + \epsilon\theta_1(u,E) + \epsilon^2\theta_2(u,E) + O(\epsilon^2), \\ k_a &= k_0(u) + \epsilon k_1(u) + \epsilon^2 k_2(u) + O(\epsilon^2). \end{aligned} \tag{4}$$

Из системы (3) получим уравнение инвариантности [2]:

$$\frac{d\theta}{d\tau} = \frac{\partial\theta}{\partial u}\frac{du}{d\tau} + \frac{\partial\theta}{\partial E}\frac{dE}{d\tau}. \tag{5}$$

Подставляя асимптотические разложения (4) в уравнение (5), с учётом уравнения медленной поверхности получим:

$$\theta_0(u,E) = \frac{\nu-E}{rk_b}e^{bE},$$

$$\theta_1(u,E) = \frac{r(uk_0(\theta_A-\theta_0)e^{-cE} - k_b\theta_0 e^{-bE})}{\beta(1-b(\nu-E))},$$

$$\theta_2(u,E) = (-\frac{1}{k_b\beta}(uk_1(\theta_A-\theta_0)e^{-cE} - uk_0\theta_1 e^{-cE} - k_b\theta_1 e^{-bE}) - \\ - \frac{\partial\theta_1}{\partial E}\theta_1 e^{-bE})\frac{rk_b}{((\nu-E)b-1)}.$$

Следует отметить, что на линии срыва $E^* = \nu - \frac{1}{b}$ выполняется соотношение $\frac{\partial\theta_0}{\partial E} = 0$. Для непрерывности полученных функций на линии срыва потребуем выполнения условий:

$$k_0(u) = \frac{e^{cE^*}}{urb(\theta_A-\theta_0(E^*))},$$

$$k_1(u) = \frac{\theta_1(E^*)e^{cE^*}}{u(\theta_A-\theta_0(E^*)}\left(uk_0e^{-cE^*} + k_be^{-bE^*} - \beta\frac{\partial\theta_1}{\partial E}(E^*)k_be^{-bE^*}\right).$$

Аналогично могут быть найдены ассимптотические разложения для инвариантной поверхности и слеивающей функции более высокого порядка.

Работа выполнена при финансовой поддержке РФФИ и Правительства Самарской области в рамках научного проекта No 16-41-630529 р_а и Министерства образования и науки Российской Федерации в рамках программы повышения конкурентоспособности Самарского университета (2013 – 2020).

Литература

1. Петренко О.Е., Нечипорук В.В., Бабюк Д.П. *Неустойчивость и осцилляции в модели электрокаталитического восстановления с учетом внешнего сопротивления цепи (квазипотенциостатический контроль)* // Электрохимия. – 1998. – Т. 34. – № 6. – С. 619–626.

2. Щепакина Е.А. Соболев В.А. *Редукция моделей и критические явления в макрокинетике*. – М.: Физматлит, 2010. – 319 с.

3. Firstova N.M., Schepakina E.A. *Modelling of Critical Conditions for an Electrochemical Reactor Model* // Procedia Engineering. – 2017. – V. 201. – P. 495–502.

4. Firstova N.M. *Conditions for the critical phenomena in a dynamic model of an electrocatalytic reaction* // Journal of Physics: Conference Series. – 2017. – V. 811. – P. 151–175.

5. Firstova N.M., Schepakina E.A. *Study of oscillatory processes in the one model of electrochemical reactor* // CEUR Workshop Proceedings. – 2016. – V. 1638. – P. 731–741.

INVARIANT SURFACE OF VARIABLE STABILITY IN THE MODEL OF THE ELECTROCATALYTIC REACTION

N.M. Firstova

The paper presents the model of the electrocatalytic reaction underlying the electrochemical reactors actions. We take the geometric approach and the theory of integral manifolds as a basis of our investigation. We construct the multidimensional invariant surface of variable stability (so-called black swan). As a result, we show that this surface consists of the canard trajectories simulating critical regimes for various initial data.

Keywords: singular perturbations, critical phenomena, canards, black swans, invariant manifold.

УДК 004.82

МЕТОД АВТОМАТИЧЕСКОГО ОПИСАНИЯ СТРУКТУРЫ ДОКУМЕНТОВ МАТЕМАТИЧЕСКОЙ КОЛЛЕКЦИИ НА ОСНОВЕ ОНТОЛОГИЙ

Ш.М. Хайдаров[1]

1 *15jkeee@gmail.com*; Казанский (Приволжский) федеральный университет, Институт математики и механики им. Н.И. Лобачевского

Описаны методы формирования семантического представления документов, которые являются частью цифровых библиотек. Данные методы основаны на онтологиях, описывающих научные документы, а также методах семантического анализа неструктурированных данных и переводе их в машиночитаемый вид.

Ключевые слова: автоматизированная обработка научных документов, семантические документы, извлечение метаданных, онтологии.

Переход к цифровой форме представления информации требует использования не только новых форматов представления самого документа, но и дополнительных данных о нем (в том числе, метаданных) с целью дальнейшей их обработки на протяжении всего жизненного цикла научной публикации. Особенности этого перехода описаны, например, в работах [1, 2]. Процесс формирования цифровых документов отличается от традиционных процессов подготовки бумажных публикаций.

Эти различия настолько велики, что переход к цифровой форме представления информации обычно называют «цифровой революцией».

В работе описан метод формирования семантического представления документов, входящих в цифровую научную коллекцию. Эта технология основана на анализе структуры документов и их стилистических особенностей. Таким образом, сделана попытка связать две технологии: обработку неструктурированных данных и перевод их в машиночитаемый вид.

Одним из современных требований к цифровым документам является возможность их семантической обработки. Чтобы научный документ был машиночитаемым, каждый его элемент должен быть размечен специальными метками, которые формируют так называемые метаданные документа. В настоящее время существует множество вариантов представления (и последующего хранения) документов с метаданными. Наиболее популярными из них являются языки семантической разметки. Одним из способов формализации такой разметки является использование онтологий. Существует множество онтологий, разработанных для разных целей, в частности, существуют онтологии для описания структуры документа [3, 4].

Традиционно цифровые научные документы хранятся в неструктурированной форме, ориентированной на макет (такой, как .pdf, .tex, .docx), поэтому такие документы сложно обрабатывать и классифицировать (см. [5, 6]). Для управления коллекциями таких документов требуется разработка дополнительных инструментов и сервисов. Наиболее типичными задачами являются: организация служб поиска, кластеризация документов, поиск похожих статей и другие. Для реализации этих сервисов необходимо использовать инструменты текстовой аналитики, в частности, методы разделения метаданных на основе структуры документов [5, 6, 7, 8, 9]. Например, в [5, 6] предложено создавать метаданные научных публикаций, с использованием регулярных выражений, а также информации о форматировании. Соответствующий алгоритм сводится к преобразованию документов из форматов .docx, .pdf в документы с XML-разметкой и к синтаксическому анализу текста на основе результатов его форматирования.

Для описания структуры научных документов разработаны специальные онтологии (см., напр., [1-4, 6, 10]. Для семантической структуризации цифрового контента в них используются онтологии SWAN, SKOS, CERIF и SPAR (см. [3, 10]). Последняя позволяет создавать комплексные машиночитаемые метаданные в формате RDF для описания любых видов документов, содержимого этих документов, а также ссылок на них. Онтологии SPAR представляют собой набор из восьми онтологий, описывающих различные типы данных (см., напр., [1, 2]). Первые четыре из них (FaBiO, CiTO, BiRO и C4O) предназначены для описания библиографических объектов научных документов и источников цитирования в списках литературы. Остальные онтологии (DoCO, PRO, PSO и PWO) служат для создания структурированных управляемых словарей для компонентов документа, публикации ролей, состояний публикации и рабочих процессов.

Онтология DoCO предоставляет множество классов и отношений, которые позволяют описывать документ на основе его структуры и содержимого. Например, она описывает подавляющее большинство компонентов документа, таких, как глава, предисловие, глоссарий и т. д. DoCO импортирует две онтологии: DEO и он-

тологию структуры документа. DEO описывает основные риторические элементы документа, кроме того, обеспечивает структурированный словарь для риторических элементов в документах и использует все риторические блочные элементы из онтологии риторики SALT. Онтология шаблонов формально определяет шаблоны для сегментирования документа на атомарные компоненты, чтобы их можно было независимо использовать в разных контекстах [1, 2, 3]. Важной частью структурного анализа документов является выделение таких блоков, как имя, фамилии авторов, их афилиации, аннотация, ключевые слова и библиографические записи.

Машинно-ориентированная обработка электронных коллекций предполагает наличие семантической разметки этих документов. Такая разметка может быть выполнена в автоматическом режиме на основе информации о структуре каждого документа и особенностях его форматирования. К таким особенностям относятся, в частности, стилевое оформление статей (шрифт, размер шрифта, выделение и т. д.), наличие ключевых слов названия элемента (например, наличие слова “Аннотации” перед блоком аннотации), расположение блока в тексте относительно других (например, документ начинается с заголовка статьи), а также совпадение по маске, что позволяет использовать технологию регулярных выражений (например, электронная почта, ФИО и т. д.) (см., например, [5, 8, 3, 11, 12, 13]).

Использование онтологий, названных выше, позволяет решать несколько дополнительных задач, таких как определение наличия ключевых конструкций и их соответствия заданному формату или преобразование коллекции в новые типы документов (макеты сборников, оглавления или другие макетоориентированные форматы).

Работа выполнена за счет средств субсидии, выделенной Казанскому федеральному университету для выполнения государственного задания в сфере научной деятельности (проект 1.2368.2017/ПЧ), и при частичной финансовой поддержке РФФИ и Правительства Республики Татарстан (проекты №№15-07-08522, 15-47-02472).

Литература

1. Peroni S. *Semantic Web Technologies and Legal Scholarly Publishing* // Springer Intern. Publ., 2014. – 304 p.

2. Peroni S. *Semantic Publishing: Issues, Solutions and New Trends in Scholarly Publishing within the Semantic Web Era* // Ph. D. Thesis. – Dep. of Comp. Sci., Univ. of Bologna, Italy, 2012. – 221 p.

3. Ruiz-Iniesta A., and Corcho O. *A Review of Ontologies for Describing Scholarly and Scientific Documents* // CEUR Workshop Proceedings. – 2014. – V. 1155. – P. 1–12.

4. Constantin A., Peroni S., Pettifer S., Shotton D., Vitali F. *The Document Components Ontology (DoCO)* // Semantic Web. – 2016. – V. 7. – No. 2. – P. 167–181.

5. Chen J., Chen H. *A Structured Information Extraction Algorithm for Scientific Papers based on Feature Rules Learning* // Journal of Software. – 2013. – V. 8. – No. 1. – P. 55—62.

6. Елизаров А.М., Липачев Е.К., Хайдаров Ш.М. *Автоматизированная система сервисов обработки больших коллекций научных документов* // Анал. и упр. данными в обл. с интенс. исп. данных: XVIII межд. конф. DAMDID / RCDL’2016. – М.: ФИЦ ИУ РАН. – 2016. – С. 109–115.

7. Biryaltsev E. V., Elizarov A.M., Zhiltsov N.G., Lipachev E.K., Nevzorova O.A., Solovyev V.D. *Methods for Analyzing Semantic Data of Electronic Collections in Mathematics* // Automatic Documentation and Mathematical Linguistics. – 2014. – V. 48. – No. 2. – P. 81—85.

8. Tkaczyk D., Tarnawski B., Bolikowski L. *Structured Affiliations Extraction from Scientific Literature* // D-Lib Magazine. – 2015. – V. 21, No. 11/12.

9. Елизаров А.М., Жижченко А.Б., Жильцов Н.Г., Кириллович А.В., Липачёв Е.К. *Онтологии математического знания и рекомендательная система для коллекций физико-математических документов* // Доклады Академии наук. – 2016. – Т. 467. – № 4. – С. 392–395.

10. Kogalovsky M.R., Parinov S.I. *Scholarly Communication in a Semantically Enrichable Research Information System with Embedded Taxonomy of Scientific Relationships* // Knowledge Engineering and Semantic Web. Comm. in Comp. and Inf. Sci., Springer. – 2015. – V. 518. – P. 87–101.

11. Елизаров А.М., Липачёв Е.К., Хайдаров Ш.М. *Семантический анализ больших коллекций научных документов* // Тр. межд. конф. по компьютерной и когнитивной лингвистике TEL–2016. – Казань: Изд-во Казан. ун-та, 2016. – С. 21–25.

12. Елизаров А.М., Липачёв Е.К., Хайдаров Ш.М. *Автоматизированная система структурной и семантической обработки физико-математического контента* // Ученые записки ИСГЗ. – 2016. – № 1 (14). – С. 210–215.

13. Хайдаров Ш.М. *Семантический анализ документов в системе управления цифровыми научными коллекциями* // Электр. библ. – 2015. – Т. 18. – № 1–2. – С. 61–85.

METHODS OF MATHEMATICAL SCIENTIFIC DOCUMENTS METADATA FORMATION BASED ON ONTOLOGIES

S.M. Khaydarov

This paper describes methods of creating semantic representation of documents that are a part of digital libraries. These methods are based on ontologies describing scientific documents, as well as methods of semantic analysis of unstructured data and their translation into machine-readable form.

Keywords: automated processing of scholarly papers, semantic documents, metadata extraction, ontologies.

УДК 517.54

КРИТЕРИЙ СУЩЕСТВОВАНИЯ ОДНОЛИСТНЫХ ОТОБРАЖЕНИЙ НА ПОЛИГОНАЛЬНЫЕ ОБЛАСТИ С ОСОБЫМ НЕОГРАНИЧЕННЫМ ВРАЩЕНИЕМ

Э.Н. Хасанова[1], П.Л. Шабалин[2]

1 *enkarabasheva@bk.ru*; Казанский государственный архитектурно-строительный университет
2 *pavel.shabalin@mail.ru*; Казанский государственный архитектурно-строительный университет

Мы исследовали однолистность конформного отображения верхней полуплоскости с фиксированным множеством прообразов вершин на полигональную область особого вида с бесконечным числом вершин и получили критерий существования однолистных отображений.

Ключевые слова: конформные отображения, однолистность, однолистные отображения, интеграл Кристоффеля-Шварца, полигональные области.

Обозначим через D_z односвязную полигональную область, которая может быть многолистной. Граница $L_z = \partial D_z$ состоит из двух ломаных: L_z^1 и L_z^2 с общей начальной точкой $A_0(0,0)$. Ломаные L_z^1 и L_z^2 имеют бесконечное число прямолинейных звеньев. Вершинами L_z^1 служат точки $A_1, A_2, \ldots$, пронумерованные последовательно от A_0, вершинами L_z^2- точки $A_{-1}, A_{-2}, \ldots$ При обходе границы области от точки A_0 вдоль ломанной L_z^1, область D_z остается слева, а вдоль L_z^2- справа. Углы, образованные действительной осью и звеньями A_0, A_1 и A_0, A_{-1} считаем заданными, без ограничения общности считаем $0 \le \eta_0^1\pi < 2\pi$, $0 < \eta_0^2\pi - \eta_0^1\pi < \pi/2$. Также, считаем известными внутренние по отношению к области D_z углы при вершинах A_k и A_{-k}, которые обозначим $\alpha_k\pi$ и $\alpha_{-k}\pi$, причем $0 < \alpha_k < 1$, $1 < \alpha_{-k} < 2$, $k = \overline{1,\infty}$. Внутренний для полигональной области D_z угол при вершине A_0 равен разности $(\eta_0^2 - \eta_0^1)\pi$.

Будем рассматривать конформные отображения $z(\zeta)$ верхней полуплоскости с двумя фиксированными монотонными последовательностями точек $\{t_k\}_{k=1}^{\infty}$, $t_k > 0$, и $\{t_{-k}\}_{k=1}^{\infty}$, $t_{-k} < 0$, на полигональную область D_z указанного вида. При отображении $z(\zeta)$ точки t_k, t_{-k} являются прообразами вершин A_k и A_{-k}, соответственно, $z(0) = 0$. Дополнительно потребуем выполнения условий

$$\sum_{k=1}^{\infty} \frac{1}{t_k} < \infty, \quad \sum_{k=1}^{\infty} \frac{1}{|t_{-k}|} < \infty. \tag{1}$$

Вводя считающие функции $n_-^*(\xi)$

$$n_-^*(\xi) = \begin{cases} 0, & 0 < \xi < -t_{-1}, \\ \sum\limits_{j=1}^{k} \kappa_{-j}, & -t_{-k} < \xi < -t_{-k-1}, \end{cases}$$

и по аналогии $n_+^*(\xi)$, где $\kappa_k = 1 - \alpha_k$, $\kappa_{-k} = \alpha_{-k} - 1$, $k = \overline{1,\infty}$, для положительных постоянных Δ, α, C потребуем выполнения следующих ограничений

$$|n_+^*(\xi) - \Delta \ln^{\alpha} \xi| < C, \quad |n_-^*(\xi) - \Delta \ln^{\alpha} \xi| < C. \tag{2}$$

Для отображения верхней полуплоскости E^+ на полигональную область с бесконечным числом вершин в случае, когда заданы величины углов при неизвестных вершинах, заданы прообразы этих вершин на вещественной оси и эти параметры удовлетворяют условиям (1), (2), в нашей работе [1] доказана формула

$$z(\zeta) = a_0 \int_0^{\zeta} \frac{e^{i\eta_0^1\pi}}{\zeta^{1-(\eta_0^2-\eta_0^1)}} \frac{\prod_{k=1}^{\infty}\left(1 - \frac{\zeta}{t_{-k}}\right)^{\kappa_{-k}}}{\prod_{k=1}^{\infty}\left(1 - \frac{\zeta}{t_k}\right)^{\kappa_k}} d\zeta. \tag{3}$$

Данная формула обобщает интеграл Кристоффеля – Шварца на случай полигональной области с бесконечным множеством вершин.

Результатом исследования вопроса об однолистности в классе отображений с фиксированными последовательностями точек $\{t_k\}_{k=1}^{\infty}$, $\{t_k\}_{k=1}^{\infty}$, удовлетворяющими условиям (1), (2), и структурной формулой (3) является следующая

Теорема. *Для того, чтобы в классе отображений (3), при условиях (1), (2) существовали однолистные необходимо и достаточно, что бы выполнялось, неравенство* $0 \le \alpha \le 1$.

Литература

1. Karabasheva E. N. Shabalin P. L. *Univalence of mappings from half-plane to a polygonal domains wiht infinite sets of vertices* // Lobachevskii J. of Math. – 2015. – V. 36, No. 2. – P. 144–153.

2. Салимов Р.Б., Шабалин П.Л. *Одно обобщение формулы Шварца-Кристоффеля* // Сиб. журн. индустр. матем. – 2010. – Т. 13, № 4. – Р. 109–117.

3. Карабашева Э.Н., Шабалин П.Л. *Об однолистности отображений обобщенной формулой Кристоффеля-Шварца* // Итоги науки и техники Серия "Совр. матем. и ее прил. Темат. обзоры". – 2017. – Т. 143. – С. 74–80.

4. Хасанова Э.Н, *Об однолистности конформных отображений обобщенным интегралом Кристоффеля-Шварца на полигональные области со счетным множеством вершин* // Изв. вузов. Математика. – 2017. – № 7. – С. 74–83.

THE CRITERIUM OF THE EXISTENCE OF UNIVALENT MAPPINGS ONTO POLIGONAL DOMAINS WITH NON-LIMITING ROTATION

E.N. Khasanova, P.L. Shabalin

We investigated univalence of the conformal mapping of the upper half-plane with a fixed set of preimages of vertices onto a special polygonal domain with an infinite number of vertices and obtained a criterium of the existence of univalent mappings.

Keywords: conformal mappings, univalence, univalent mappings, Schwartz Christoffel integral, polygonal domains.

УДК 517.54

НЕОДНОРОДНАЯ КРАЕВАЯ ЗАДАЧА ГИЛЬБЕРТА С КОНЕЧНЫМ ЧИСЛОМ ТОЧЕК РАЗРЫВА ВТОРОГО РОДА

П.Л. Шабалин[1], А.Х. Фатыхов[2]

1 *pavel.shabalin@mail.ru*; Казанский государственный архитектурно-строительный университет
2 *vitofat@gmail.ru*; Казанский государственный архитектурно-строительный университет

В статье рассматривается неоднородная краевая задача Гильберта теории аналитических функций с бесконечным индексом для полуплоскости. Коэффициенты краевого условия непрерывны по Гельдеру всюду, кроме конечного числа особых точек, в которых аргумент функции коэффициентов имеет разрывы второго рода (степенного порядка с показателем меньше единицы). Получены формулы общего решения неоднородной задачи, рассмотрены вопросы существования и единственности решения. При исследовании решения применялся аппарат теории целых функций и геометрической теории функций комплексного переменного.

Ключевые слова: задача Гильберта, принцип Фрагмена - Линделефа, бесконечный индекс, целые функции.

1. Постановка задачи

Пусть $E^+ = \{z : z = x + iy,\ 0 < y\}$ – верхняя полуплоскость в плоскости комплексного переменного z, $L = \partial E^+$. Рассмотрим краевую задачу Гильберта теории анали-

тических функций с краевым условием на вещественной оси

$$a(t)\,\mathrm{Re}\,\Phi(t) - b(t)\,\mathrm{Im}\,\Phi(t) = c(t),\ t \in L.$$

Мы впервые рассматриваем неоднородную задачу Гильберта для полуплоскости с конечным числом точек двустороннего завихрения. Здесь коэффициенты краевого условия неоднородной задачи Гильберта непрерывны по Гельдеру всюду на вещественной оси кроме конечного числа особых точек $t_0 = \infty$ и t_j, $j = \overline{1,n}$, в которых аргумент функции коэффициентов ($\arg[a(t) - ib(t)]$) имеет разрывы второго рода степенного порядка.

Запишем краевое условие задачи Гильберта в виде

$$\mathrm{Re}[e^{-i\nu(t)}\Phi(t)] = \frac{c(t)}{|G(t)|}, \quad t \in L,\ t \neq t_j, j = \overline{1,n}, \tag{1}$$

где $G(t) = a(t) - ib(t)$, причем $a^2(t) + b^2(t) \neq 0$ всюду на L и функция $\nu(t) = \arg G(t)$, непрерывна на L всюду, кроме точек t_0, t_j, $j = \overline{1,n}$, в которых она имеет разрывы второго рода. Именно, справедливо представление

$$\nu(t) = \sum_{j=0}^{n} \nu_j(t) + \widetilde{\nu}(t),$$

$$\nu_0(t) = \begin{cases} \nu^- t^\rho, & t > 0, \\ \nu^+ |t|^\rho, & t < 0, \end{cases} \qquad \nu_j(\theta) = \begin{cases} \dfrac{\nu_j^-}{(t_j - t)^{\rho_j}}, & t < t_j, \\ \dfrac{\nu_j^+}{|t_j - t|^{\rho_j}}, & t_j < t, \end{cases} \qquad j = \overline{1,n},$$

с некоторыми числами ν^+, ν^-, ν_j^+, ν_j^-, ρ, $0 < \rho < 1$, ρ_j, $0 < \rho_j < 1$, $j = \overline{1,n}$, функция $\widetilde{\nu}(t) \in H_L(\mu)$. Здесь $H_L(\mu)$– класс функций $\widetilde{\nu}(t)$, удовлетворяющих условию Гельдера с показателем μ на всем контуре L, включая бесконечно удаленную точку. Также считаем, $|G(t)| \in H_L(\mu)$, $c(t) \in H_L(\mu)$.

Вначале получим формулу общего решения и исследуем разрешимость однородной задачи, то есть определим функцию $\Phi(z)$, аналитическую и ограниченную в области E^+ по краевому условию

$$\mathrm{Re}[e^{-i\nu(t)}\Phi(t)] = 0, \quad t \in L,\ t \neq t_j, j = \overline{1,n}.$$

Отметим, что общее решение и некоторые результаты по разрешимости однородной задачи Гильберта на окружности с конечным числом точек двустороннего завихрения получены в [1].

2. Решение однородной задачи

Теорема 1. *Общее решение однородной краевой задачи в классе ограниченных в E^+ функций дается формулой*

$$\Phi(z) = -ie^{i\Gamma(z)} \exp\{il e^{i\alpha} z^\rho\} \prod_{j=1}^{n} \exp\left\{i \frac{l_j e^{i\alpha_j}}{(t_j - t)^{\rho_j}}\right\} F(z), \tag{2}$$

где $F(z)$ произвольная аналитическая в E^+ функция, удовлетворяющая неравенствам

$$\begin{cases} |F(z)| \le C_1 e^{C_2/|t_j - z|^{\rho_j}}, \ z \to t_j, \ z \in E^+, \ 0 < \rho_j < 1, \ j = \overline{1,n}, \\ |F(z)| \le C_1 e^{C_2|z|^{\rho}}, \ z \to \infty, \ z \in E^+, \ 0 < \rho < 1, \end{cases}$$

и на границе L условиям

$$\operatorname{Im} F(t) = 0, \quad t \in L, \quad t \ne t_j,$$

$$|F(t)| \le C \exp\Big\{Q_0(t) + \sum_{j=1}^{n} Q_j(t)\Big\}, \quad C = \text{const}, \ t \in L.$$

3. Условия разрешимости однородной задачи

Теорема 2. *Однородная краевая задача*
а) не имеет нетривиальных ограниченных решений, если выполнены условия

$$\nu_j^- \cos(\pi\rho_j) - \nu_j^+ \le 0, \quad \nu_j^- - \nu_j^+ \cos(\pi\rho_j) \le 0, \quad j = \overline{1,n},$$

причем хотя бы одно из неравенств строгое;

b) имеет единственное решение вида $\Phi(z) = -iAe^{\Gamma(z)}$, $A = \text{const}, \operatorname{Im} A = 0$, если $\nu_j^- \cos(\pi\rho_j) - \nu_j^+ = 0$, $\nu_j^- - \nu_j^+ \cos(\pi\rho_j) = 0$, $j = \overline{1,n}$.

Теперь рассмотрим следующие однородные задачи Гильберта для полуплоскости E^+ с двусторонним завихрением степенного порядка в единственной точке:

$$\operatorname{Re}[e^{-i\nu_0(t)}\Phi_0(t)] = 0, \quad t \in L, \quad \nu_0(t) = \begin{cases} \nu^- t^{\rho}, \ t > 0, \\ \nu^+ |t|^{\rho}, \ t < 0, \end{cases} \tag{3}$$

$$\operatorname{Re}[e^{-i\nu_j(t)}\Phi_j(t)] = 0, \quad t \in L, \ t \ne t_j, \quad \nu_j(\theta) = \begin{cases} \dfrac{\nu_j^-}{(t_j - t)^{\rho_j}}, \ t < t_j, \\ \nu_j^+ \\ \dfrac{\nu_j^+}{|t_j - t|^{\rho_j}}, \ t_j < t, \end{cases} \quad j = \overline{1,n}, \tag{4}$$

4. Решение неоднородной задачи

Теорема 3. *Если задачи (3) и (4) для всех $j = \overline{1,n}$ имеют бесконечное множество решений каждая, то общее решение неоднородной краевой задачи (1) представляется как сумма функций (2) и*

$$\Phi(z) = -ie^{i\Gamma(z)} \exp\{ile^{i\alpha} z^{\rho}\} \prod_{j=1}^{n} \exp\Big\{i\frac{l_j e^{i\alpha_j}}{(t_j - t)^{\rho_j}}\Big\} \tilde{F}(z) \frac{1}{\pi} \int_L \frac{c_1(t)dt}{t - z}.$$

.

Работа выполнена при финансовой поддержке фонда РФФИ (проект № 17-01-00282-а)

Литература

1. Salimov R.B., Fatykhov A.Kh., Shabalin P.L. *Homogeneous Hilbert boundary value problem with several points of turbulence* // Lobachevskii J. of Math. – 2017. – V. 38, No. 3. – P. 414–419.

HOMOGENEOUS HILBERT BOUNDARY VALUE PROBLEM
WITH SEVERAL POINTS OF TURBULENCE

P.L. Shabalin, A.Kh. Fatykhov

In the upper half-plane we consider the Riemann-Hilbert boundary-value problem with infinite index. Its coefficient is Holder continuous everywhere, except of a finite set of points, where its argument has discontinuities of the second order. We investigate existence and uniqueness of solution and describe the set of solutions in the case of nonuniqueness. Our methodology is based on the theory of entire functions and the geometric theory of functions.

Keywords: Riemann-Hilbert boundary value problem, existence, uniqueness of solution, entire functions, infinite index.

УДК 514.76

О ДВУХ ОХВАТАХ ФУНДАМЕНТАЛЬНО-ГРУППОВОЙ СВЯЗНОСТИ НА ПОВЕРХНОСТИ АФФИННОГО ПРОСТРАНСТВА

А.В. Шульц[1]

1 *tonja92@mail.ru*; Балтийский Федеральный университет им. И. Канта, Институт физико-математических наук и информационных технологий

Получено два охвата объекта фундаментально-групповой связности. Найдены аналитические и геометрические условия совпадения двух типов охватов.

Ключевые слова: поверхность аффинного пространства, фундаментально-групповая связность, оснащение.

Рассмотрим n-мерное аффинное пространство A_n с подвижным репером $\{A, \bar{e}_I\}$, пусть $\bar{A}$ – радиус-вектор точки A, исходящей из некоторого центра. Перемещения репера задаются формулами:

$$d\bar{A} = \omega^I \bar{e}_I, \;\; d\bar{e}_I = \omega_I^J \bar{e}_J \;\; (I, J, K... = \overline{1, n}).$$

Базисные формы ω^I, ω_I^J аффинной группы $GA(n)$, $\dim GA(n) = n(n+1)$, действующей в пространстве A_n, удовлетворяют уравнениям Картана:

$$D\omega^I = \omega^J \wedge \omega_J^I, \;\; D\omega_J^I = \omega_J^K \wedge \omega_K^I.$$

Рассмотрим m-мерную поверхность S_m $(1 \le m < n)$ в аффинном пространстве A_n. Произведем специализацию репера $R = \{A, \bar{e}_i, \bar{e}_\alpha\}$ $(i, j, k... = \overline{1, m};\ \alpha, \beta, \gamma... = \overline{m+1, n})$ следующим образом: поместим вершину A в текущую точку поверхности S_m, а векторы $\bar{e}_i$ – в соответствующую касательную плоскость T_m. Уравнения поверхности S_m в адаптированном репере будут иметь вид:

$$\omega^\alpha = 0, \;\; \omega_i^\alpha = \Lambda_{ij}^\alpha \omega^j.$$

Замыкая первую подсистему, получим $\Lambda^{\alpha}_{ij} = \Lambda^{\alpha}_{ji}$. Продолжая вторую подсистему, получим

$$\triangle\Lambda^{\alpha}_{ij} = \Lambda^{\alpha}_{ijk}\omega^k,$$

т. е. функции Λ^{α}_{ij} образуют тензор, который называется фундаментальным тензором поверхности S_m.

Оснащение поверхности S_m состоит в присоединении к каждой точке $(n-m)$-мерной плоскости N_{n-m}: $T_m + N_{n-m} = A_n$. Нормаль N_{n-m} зададим совокупностью векторов $\bar{E}_\alpha = \bar{e}_\alpha + \lambda^i_\alpha \bar{e}_i$.

Уравнения инвариантности нормали имеют вид:

$$\triangle\lambda^i_\alpha + \omega^i_\alpha = \lambda^i_{\alpha j}\omega^j \quad (\triangle\lambda^i_\alpha = d\lambda^i_\alpha + \lambda^j_\alpha\omega^i_j - \lambda^i_\beta\omega^\beta_\alpha).$$

Продолжая их, найдем уравнения на пфаффовы производные $\lambda^i_{\alpha j}$ оснащающего квазитензора λ^i_α:

$$\triangle\lambda^i_{\alpha j} + \lambda^k_\alpha\omega^i_{kj} - \lambda^i_\beta\omega^\beta_{\alpha j} = \lambda^i_{\alpha jk}\omega^k.$$

где $\omega^i_{jk} = \Lambda^\alpha_{jk}\omega^i_\alpha$, $\omega^\alpha_{\beta k} = -\Lambda^\alpha_{ik}\omega^i_\beta$.

Фундаментальный тензор $\Lambda = \{\Lambda^\alpha_{ij}\}$ и оснащающий квазитензор $\lambda = \{\lambda^i_\alpha\}$ позволяют охватить объект ассоциированной фундаментально-групповой связности Γ двумя способами: $\overset{1}{\Gamma} = \{\overset{0}{\Gamma}{}^i_{jk}, \overset{0}{\Gamma}{}^\alpha_{\beta i}, \Gamma^i_{\alpha j}\}$ и $\overset{2}{\Gamma} = \{\overset{0}{\Gamma}{}^i_{jk}, \overset{0}{\Gamma}{}^\alpha_{\beta i}, \Gamma^i_{\alpha j}\}$ [1], причем объекты индуцированной аффинной и нормальной линейной связностей удовлетворяют условию:

$$\overset{0}{\Gamma}{}^i_{jk}\,\lambda^k_\alpha + \overset{0}{\Gamma}{}^\beta_{\alpha j}\,\lambda^i_\beta = 0.$$

Теорема 1. *Два типа охватов совпадают в том и только в том случае, когда* $\lambda^i_{\alpha j} = \Lambda^\beta_{jk}\lambda^k_\alpha\lambda^i_\beta$.

Теорема 2. *Альтернации ковариантных производных компонент объектов фундаментально-групповой связности первого типа равны соответствующим компонентам тензора кривизны, а для второго типа обращаются в нуль.*

Литература

1. Сыроквашина А. Н. *Параллельные перенесения нормали поверхности аффинного пространства* // Диф. геом. многообр. фигур. – Калининград. – 1999. – Вып. 30. – С. 84–88.

ABOUT TWO SCOPES OF THE FUNDAMENTAL-GROUP CONNECTION ON SURFACE OF THE AFFINE SPACE

A.V. Shults

Two scopes of the fundamental-group connection object were obtained. The analytical and geometric conditions for the coincidence of two types of scopes are found.

Keywords: surface of affine space, fundamental-group connection, framing.

УДК 517.544.8

ПОСТРОЕНИЕ ПРИБЛИЖЕННОГО РЕШЕНИЯ ДВУМЕРНОЙ ЗАДАЧИ ДИРИХЛЕ В ДВУСВЯЗНЫХ ОБЛАСТЯХ ВБЛИЗИ ГРАНИЦ

А. Эльшенави[1], Е.А. Широкова[2]

1 *atallahtm@yahoo.com*; Казанский (Приволжский) федеральный университет, Институт математики и механики им. Н.И. Лобачевского

2 *elena.shirorova@kpfu.ru*; Казанский (Приволжский) федеральный университет, Институт математики и механики им. Н.И. Лобачевского

Предлагается метод приближенного решения двумерной задачи Дирихле для уравнения Лапласа в двусвязных областях с помощью интеграла Коши. Гармоническая функция вблизи границ аппроксимируется линейной функцией.

Ключевые слова: интеграл Коши, двумерная задача Дирихле, двусвязная область.

Пусть Ω – двусвязная область, $\partial\Omega = L_0 \cup L_1$ – гладкая граница этой области. Предположим, что граница состоит из внешней гладкой кривой $L_0 : z_0(t), t \in [0, 2\pi]$, обходящейся с ростом t в направлении против часовой стрелки, и внутренней гладкой кривой $L_1 : z_1(t), t \in [0, 2\pi]$, обходящейся по часовой стрелке. Тогда соответствующая двумерная задача Дирихле для уравнения Лапласа состоит в том, чтобы найти дважды дифференцируемую в Ω функцию $u(x, y)$, непрерывную в $\Omega \cup \partial\Omega$ и удовлетворяющую уравнению Лапласа

$$\frac{\partial^2 u(x,y)}{\partial x^2} + \frac{\partial^2 u(x,y)}{\partial y^2} = 0, \qquad (x, y) \in \Omega, \tag{1}$$

и граничным условиям:

$$u(x(t), y(t)) = \begin{cases} f_0(t), & (x(t), y(t)) \in L_0; \\ f_1(t), & (x(t), y(t)) \in L_1; \end{cases} \qquad t \in [0, 2\pi]. \tag{2}$$

В [1] решение этой проблемы искалось в виде интеграла Коши. Метод сводит задачу к интегральному уравнению Фредгольма второго рода для граничных значений сопряженной гармонической функции и затем преобразует интегральное уравнение в усеченную линейную систему. Решение интегрального уравнения имеет вид полиномов Фурье. Наконец, решение задачи Дирихле является действительной частью интеграла Коши. Из-за сингулярности интеграла Коши в точках вблизи границ мы вводим новую технику для построения приближенного решения в этих точках. Приближенным решением задачи Дирихле в точках вблизи границ является линейная функция.

Определим конгруентные границам кривые, показанные на рис. 1:

$$z_{\varepsilon j}(t) = z_j(t) + 0.5 i R_j \frac{z_j'(t)}{|z_j'(t)|}, \quad j = 0, 1,$$

Здесь R_j, $j = 0, 1$ – минимальное значение радиусов кривизны граничных с уравнениями кривых $z_j(t), j = 0, 1$. Обозначим приближенное решение в точках кривых $z_{\varepsilon j}(t), j = 0, 1$, вычисленное методом интеграла Коши, через $u_{\varepsilon j}(t)$, $j = 0, 1$, $t \in [0, 2\pi]$.

Обозначим через $\tilde{\Omega}$ область с границами $z_{\varepsilon j}(t)$. Для точек области $\Omega \setminus \tilde{\Omega}$, решение задачи Дирихле аппроксимируется линейными функциями следующим образом.

Во-первых, мы строим для каждой точки, расположенной между конгруентными кривыми $z_j(t)$ и $z_{\varepsilon j}(t)$, отрезок прямой, перпендикулярной конгруентным кривым $z_j(t)$ и $z_{\varepsilon j}(t)$ и обеспечивающий проекции точки на эти кривые: $z_j(t_0)$ и $z_{\varepsilon j}(t_0)$.

Во-вторых, вычисляем приближенное решение задачи Дирихле в этой точке путем подстановки в уравнениях прямых следующим образом:

$$u_\zeta = \frac{u_{\varepsilon j}(t_0) - f_j(t_0)}{z_{\varepsilon j}(t_0) - z_j(t_0)} \big(\zeta - z_j(t_0)\big) + f_j(t_0), \quad j = 0, 1. \tag{3}$$

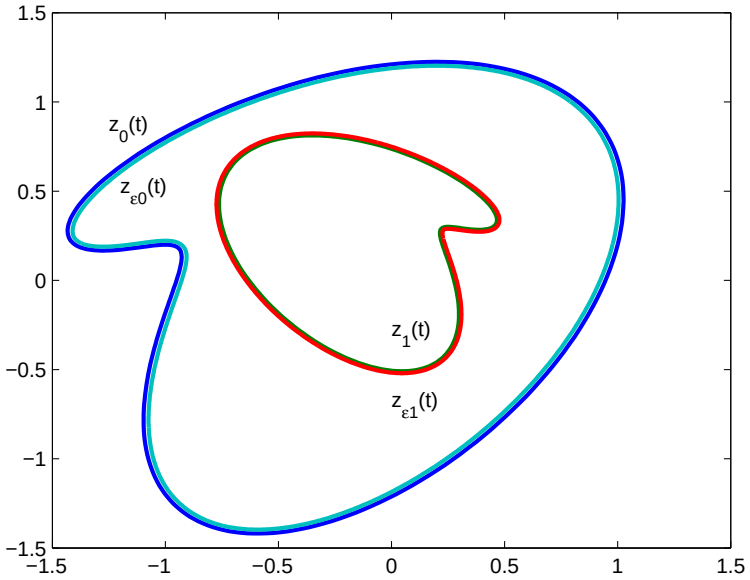


Рис. 1. Граничные кривые $z_j(t)$ и $z_{\varepsilon j}(t)$, $j = 0, 1$.

Интегральный метод Коши в сочетании с предлагаемой техникой был применен к двусвязной области с незвездными границами, показанными на рисунке (1). Границы состояли из двух параметрических кривых:

$$z_0(t) = -0.5 + e^{it} + 0.5e^{2it} + 0.2ie^{-2it}, \qquad t \in [0, 2\pi],$$

$$z_1(t) = 0.2i + 0.5e^{-it} - 0.25e^{-2it} + 0.1ie^{2it}, \qquad t \in [0, 2\pi].$$

Полная область с контурными графиками решения двумерного уравнения Лапласа с постоянными граничными значениями показана на рис. 2.

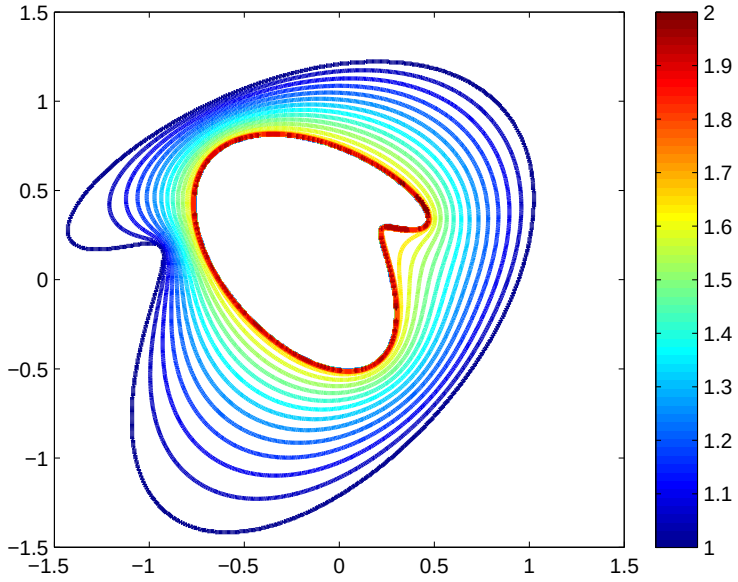


Рис. 2. Контурный график гармонической функции решения двумерного уравнения Лапласа с постоянными граничными значениями.

Литература

1. Elshenawy A., Shirokova E. A. Dirichlet problem solution for simply and doubly connected domains with smooth boundaries// Тр. Матем. центра им. Н. И. Лобачевского. – Казань: Изд-во Казан. матем. об-ва, 2017. – Т. 54. – С. 12–15.

CONSTRUCTION OF THE APPROXIMATE SOLUTION OF 2D DIRICHLET PROBLEM IN DOUBLY CONNECTED DOMAINS NEAR THE BOUNDARIES

A. Elshenawy, E.A. Shirokova

The method constructs an approximate Cauchy integral solution of the 2D Dirichlet problem in doubly connected domains. The harmonic function near the boundaries is approximated by linear functions.

Keywords: Cauchy integral, 2D Dirichlet problem, doubly connected domain.

УДК 532.3

МОДЕЛИРОВАНИЕ ДВИЖЕНИЯ ДВУХМАССОВОГО КЛИНОВИДНОГО ВИБРОРОБОТА В ВЯЗКОЙ ЖИДКОСТИ

А.И. Юнусова[1]

1 *yunusova24@rambler.ru*; Казанский национальный исследовательский технологический университет

В данной работе исследуется движение двухмассовой вибрационной системы (виброробот) в вязкой жидкости. Система состоит из герметичного клиновидного корпуса и подвижной внутренней массы. Рассматриваются вопросы повышения эффективности движения виброробота. Решение задачи выполняется численно на базе пакета с

открытым программным кодом OpenFOAM.

Ключевые слова: виброробот, вязкая жидкость, эффективность движения, OpenFOAM.

Вибрационный принцип движения тел вызывает интерес у инженеров уже многие годы. Начиная с первой половины 20 века в технической литературе было описано множество устройств с вибрационным движителем. Вибрационное движение в последние годы является предметом всестороннего исследования в прикладной механике и робототехнике [1-4].

В данной работе рассматривается прямолинейное движение двухмассовой системы в вязкой несжимаемой жидкости области низких чисел Рейнольдса. Система состоит из герметичного клиновидного корпуса массы M и подвижной внутренней массы m. Перемещение системы происходит за счет продольного периодического движения внутренней массы относительно корпуса. Данный принцип передвижения представляется целесообразным для мини- и микро-устройств.

Уравнение движения системы записывается в следующем виде:

$$\dot{u}_M = -\mu_2 \dot{u}_m + \mu_1 \frac{R^2}{S} F.$$

Здесь μ_2 – отношение подвижной массы к полной массе виброробота, μ_1 – отношение массы вязкой жидкости, занимающей тотже объем, что и виброробот, к массе виброробота, S – площадь поперечного сечения корпуса.

Движение жидкости вокруг виброробота описывается системой уравнений Навье-Стокса. Эту систему уравнений в декартовой системе координат можно записать как:

$$\frac{\partial U}{\partial t} + U \cdot \nabla U = -\nabla p + \frac{1}{Re} \Delta U, \nabla \cdot U = 0,$$

где $U = (u, v)$ – безразмерная скорость, p – безразмерное давление, Re – число Рейнольдса.

Вычисление сил, действующих на корпус виброробота со стороны вязкой жидкости, в безразмерной постановке проводится по формуле:

$$F = \int_\Omega p n ds - \int_\Omega \overline{\sigma} \cdot n ds,$$

где $\overline{\sigma}$ – тензор вязких напряжений, Ω – поверхность виброробота, n – внешняя нормаль к поверхности виброробота.

Задача взаимодействия робота с вязкой жидкостью решается с помощью прямого численного моделирования, проводимого в открытом пакете OpenFOAM на базе схемы, представленной в [5].

В работе исследуются вопросы повышения эффективности и скорости движения устройства за счет выбора специального закона перемещения внутренней массы. Для этого проводится сравнительный анализ характеристик движения и режимов обтекания при простом гармоническом законе колебания внутренней массы и специальном двухфазном, полученном в [4]. В обоих случаях рассматривается периодическое движение, происходящее вдоль оси симметрии корпуса виброробота.

Результаты исследования показывают, что направленное движение виброро-

бота с клиновидной формой корпуса возможно реализовать как для гармонического, так и для двухфазного законов движения внутренней массы. Для случая гармонического закона движение системы при одинаковых параметрах колебания внутренней массы, возможно как основанием вперед так и вперед вершиной, выбор направления движения определяется начальными условиями. Двухфазный закон колебания внутренней массы обеспечивает единственное возможное направление движения системы. Максимальные характеристики достигаются при перемещении робота вперед вершиной. Используя двухфазный закон, можем обеспечить более высокую скорость движения (до 50%) в жидкости, а также значительно увеличить эффективность движения (до 3 раз).

Работа выполнена при финансовой поддержке РФФИ 16-31-00462 (мол_а)

Литература

1. Черноусько Ф.Л. *Оптимальные периодические движения двухмассовой системы в сопротивляющейся среде* // ПММ. – 2008. – Т. 72. – Вып. 2. – С. 202–215.

2. Болотник Н. Н., Фигурина Т. Ю., Черноусько Ф. Л. *Оптимальное управление прямолинейным движением системы двух тел в сопротивляющейся среде* // ПММ. – 2012. – Т. 76. – Вып. 1. – С. 3–22.

3. Егоров А. Г., Захарова О. С. *Оптимальное по энергетическим затратам движение виброробота в среде с сопротивлением* // ПММ. – 2010. – Т. 74. – Вып. 4. – С. 620–632.

4. Егоров А. Г., Захарова О. С. *Оптимальное квазистационарное движение виброробота в вязкой жидкости* // Изв. вузов. Математика. – 2012. – Вып. 2. – С. 57–64.

5. Нуриев А. Н., Захарова О. С. *Численное моделирование движения клиновидного двухмассового виброробота в вязкой жидкости* // Вычисл. мех. спл. сред. – 2016. – Т. 9. – No 1. – С. 5–15.

SIMULATION OF THE MOTION OF A TWO-MASS WEDGE-SHAPED VIBRATION-DRIVEN ROBOT IN A VISCOUS FLUID

A.I. Yunusova

This paper is devoted to the study of the two-mass vibration-driven system motion in the viscous fluid. The system consists of a closed wedge-shaped body, placed in a fluid, and a movable internal mass. The problems of increasing of the efficiency of vibration-driven robot movement are considered. The numerical solution of the problem is carried out in the OpenFOAM package.

Keywords: vibration-driven robot, viscous fluid, motion efficiency, OpenFOAM.

УДК 004.42

ФОРМИРОВАНИЕ СЛОВАРЯ РЕКОМЕНДАТЕЛЬНОЙ СИСТЕМЫ АВТОМАТИЧЕСКОГО ПОДБОРА УДК

Г.Ш. Ямалутдинова[1]

1 *yamalytdinova@mail.ru*; Казанский (Приволжский) федеральный университет, Институт математики и механики им. Н.И. Лобачевского

Рассмотрены наиболее известные классификаторы, предназначенные для систематизации научной информации. Предложено использование рекомендательной системы

для автоматизации процесса классификации и меры Танимото для оценки близости слов. Приведен алгоритм формирования словаря классификатора УДК. Представлен вариант реализации сервиса автоматического подбора УДК.

Ключевые слова: рекомендательная система, классификатор, УДК, систематизация научной информации.

В связи с ростом научной информации ее систематизация имеет особую значимость. Наиболее известными классификаторами, которые используют во всем мире, являются Универсальная десятичная классификация (УДК) [1], Библиотечно-библиографическая классификация (ББК) [2], Математическая предметная классификация (последняя версия MSC2010) [3]. Из-за большого объема таблиц ручной подбор индекса классификатора – длительный и трудоёмкий процесс. Необходимо знать структуру таблиц, понимать принцип составления индексов. Автоматизация данного процесса является важной задачей. Одно из решений – создание рекомендательной системы, роль таких систем в последнее время заметно возросла (см., напр., [4]).

В [5] предложен алгоритм автоматического подбора индексов классификатора УДК на основе анализа названия статьи и списка ключевых слов, представленных автором. Данная работа является развитием [6]. Она посвящена формированию словаря классификатора, позволяющего более точно определить область исследований и подобрать индекс классификатора. На основе данных алгоритм пополнения словаря состоит из следующих пунктов:

1) анализ статей с указанным УДК и ключевыми словами;

2) выделение терминов из текста статей;

3) использование онтологии (см., напр., [7]).

Были проанализированы статьи с сайта Math-Net.ru [8], в которых указан УДК и блок ключевых слов. С этой целью написаны скрипты, которые из html-страниц выделяют необходимые метаданные: название статьи, УДК и список ключевых слов. Из-за машинной обработки полученые данные имеют некоторые неточности. Например, у некоторых журналов разметка для индекса УДК отличается или в названии статьи присутствуют символы html-разметки. Для уменьшения неточностей была произведена дополнительная обработка. Результат был записан в XML-представление, разработанное в [6].

Алгоритм автоматического подбора УДК реализован в виде сервиса, который использует название и ключевые слова статьи.

Система сравнивает введеные данные с терминами, представленными в словаре, при этом использует меру Танимото

$$T = \frac{N_c}{N_a + N_b - N_c}, \; T \in (0, 1), \tag{1}$$

где T – коэффициент схожести, N_a – количество элементов в первом множестве, N_b – количество элементов во втором множестве, N_c – количество общих элементов в обоих множествах.

```
<UDC id="51" title="МАТЕМАТИКА">
    <item id="510">
        <title>Фундаментальные и общие проблемы математики</title>
        <keywords/>
        <references></references>
        <parent>51</parent>
    </item>
    <item id="510.2">
        <title>Общие проблемы математической логики и оснований математики</title>
        <keywords/>
        <references></references>
        <parent>510</parent>
    </item>
    <item id="510.3">
        <title>Теория множеств</title>
        <keywords/>
        <references></references>
        <parent>510</parent>
    </item>
    <item id="510.5">
        <title>Теория вычислимости</title>
```

Рис. 1. XML-представление УДК

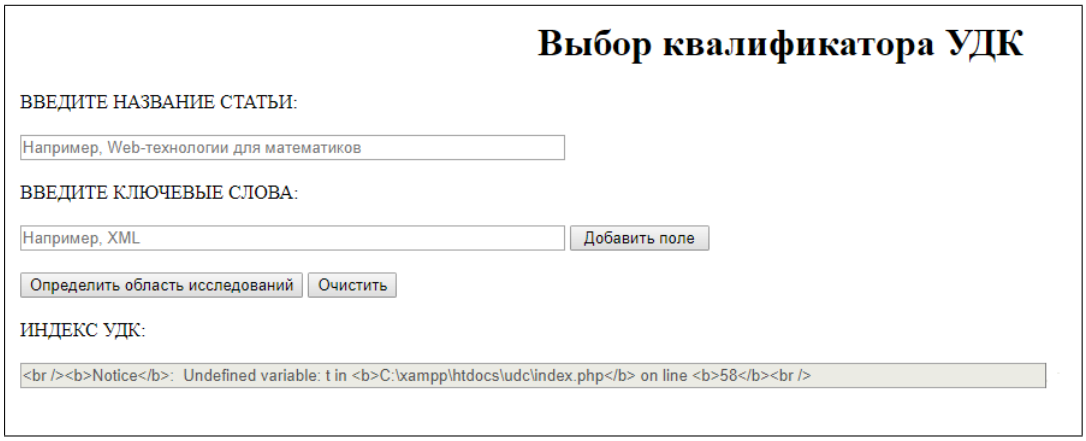


Рис. 2. Сервис автоматического подбора УДК

Индекс, который имеет наибольший коэффициент схожести, рекомендуется в качестве классификатора для статьи.

В заключении отметим, что нами рассмотрены наиболее известные системы классификации научной информации. Представлен и реализован алгоритм формирования словаря УДК. Сформирован словарь терминов. Выбрана мера Танимото для оценки близости слов. Создан сервис автоматического подбора классификатора.

Работа выполнена за счет средств субсидии, выделенной Казанскому федеральному университету для выполнения государственного задания в сфере научной деятельности (проект 1.2368.2017/ПЧ), и при частичной финансовой поддержке РФФИ и Правительства Республики Татарстан (проект №№15-07-08522, 15-47-02472).

Литература

1. UDC SummaryLinkedData. http://udcdata.info/.

2. *Библиотечно-библиографическая классификация*. http://roslavl.library67.ru/files/382/bbk.pdf.

3. *Классификатор математических сущностей MSC2010*. http://www.ams.org/mathscinet/msc/msc2010.html

4. Елизаров А.М., Жижченко А.Б., Жильцов Н.Г., Кириллович А.В., Липачёв Е.К. *Онтологии математического знания и рекомендательная система для коллекций физико-математических документов* // Докл. РАН. – 2016. – Т. 467, № 4. – С. 392–395.

5. Ямалутдинова Г.Ш. *Алгоритм автоматического подбора классификаторов физико-математических публикаций* // Труды Матем. центра им. Н. И. Лобачевского. – 2016. – Т. 53. – С. 172–174.

6. Ямалутдинова Г.Ш. *Алгоритм формирования словарей рекомендующей системы подбора классификаторов научной информации* // Уч. записки ИСГЗ. – 2017. – № 1(15). – С. 552–557.

7. Nevzorova O.A., Zhiltsov N., Kirillovich A., Lipachev E. *OntoMathPRO ontology: A linked data hub for mathematics*. In: Klinov P., Mouromtsev D. (eds). Knowledge Engineering and the Semantic Web. KESW 2014.Communications in Computer and Information Science. — 2014. – V. 468. – P. 105–119.

8. Math-Net.ru http://www.mathnet.ru/

9. Řehůřek R., Sojka P. *Automated Classification and Categorization of Mathematical Knowledge* // Lecture Notes in Artificial Intelligence. – 2008. – 5144. – P. 543–557.

FORMING A DICTIONARY OF THE RECOMMENDED AUTOMATIC SELECTION SYSTEM UDC

G.S. Yamalytdinova

We consider the most popular classifiers for systematization of scientific information. There are proposed the using recommender system for automation of the classification process and Tanimoto's measure for proximity evaluation. We give an algorithm of forming classificator's dictionary. There is a version of the automatic selection for the UDC service.

Keywords: recommendatory system, classifier, UDC, systematization of scientific information.

UDC 517.98

ON SOME OPERATOR INEQUALITIES

A.A. Sami[1]

1 *samialbarkish@gmail.com*; Kazan Federal University

We prove some operator inequalities for a Hilbert space.

Keywords: Hilbert space, linear operator, projection, operator inequality, hyponormal operator.

Let $B(H)$ be a *- algebra of all bounded linear operators on a Hilbert space H, I be the identity operator. An operator $a \in B(H)$ is hyponormal if $a^*a \geq aa^*$ [1]. Let $B(H)^{pr} = \{p \in B(H) : p = p^2 = p^*\}$.

Theorem 1. *Let $x, y \in B(H)$ and $z = x + y$. Then $x^*x + \Re(z^*y) = y^*y + \Re(z^*x) \geq \frac{3}{4}z^*z$. We have also $x^*x + \Re(z^*y) \geq \frac{3}{4\text{Ĺ}}y^*y$.*

Corollary 1. *Let $x, y \in B(H)$ and $z = x + y$.*

i. We have $x^*x + \Re(z^*y) \geq \frac{3}{4\text{Ĺ}}(\lambda y^*y + (1-\lambda)z^*z)$ for all $0 \leq \lambda \leq 1$.

ii. If y (or z) is left invertible, then $x^*x + \Re(z^*y)$ is invertible.

iii. We have $y^* y \geq \epsilon I$ *(or* $z^* z \geq \epsilon I$ *) for some number* $\epsilon > 0$*. Thus,* $x^* x + \Re(z^* y) \geq \frac{3\epsilon}{4}I$.

Theorem 2. *Let* $x, y \in B(H)$ *and* $z = x + y$*. Then for all numbers* $a, b > 0$ *we have* $(1-a)x^* x + (1 - \frac{1}{a})y^* y \leq z^* z \leq (1+b)x^* x + (1 + \frac{1}{b})y^* y$.

Via Theorem 1 and 2 we have

Corollary 2. *Let* $x, y \in B(H)$ *and* $z = x + y$ *. Then for all* $a > 0$ *we have*

$$x^* x + \Re(z^* y) = y^* y + \Re(z^* x) \geq \frac{3}{4}((1-a)x^* x + (1 - \frac{1}{a})y^* y).$$

Theorem 3. *Suppose* $p, q \in B(H)^{pr}$ *and* $a = p + \lambda p$ *with* $\lambda \in \mathbb{C}\ \mathbb{R}$*, then the following conditions are equivalent:*

i an operator $a^* a - a a^*$ *is invertible;*

ii the operators $p - q$ *,* $p^{\perp} - q$ *are invertible.*

Under this conditions operator a is invertible.

Theorem 4. *Suppose* $b \in B(H)^{sa}$*,* $q \in B(H)^{pr}$*,* $a = b + \lambda q$ *with* $\lambda \in \mathbb{C} \setminus \mathbb{R}$.
Then the following conditions are equivalent:

i. an operator a is hyponormal;

ii. $bq = qb$.

Under this conditions an operator a is normal.

References

1. Halmos P.R. *A Hilbert space problem book.* – D. Van Nostrand company, Inc., London, 1967.

АВТОРСКИЙ УКАЗАТЕЛЬ

ТРУДЫ
МАТЕМАТИЧЕСКОГО ЦЕНТРА
ИМЕНИ Н. И. ЛОБАЧЕВСКОГО

ТОМ 55

ЛОБАЧЕВСКИЕ ЧТЕНИЯ – 2017

Материалы Шестнадцатой молодежной школы-конференции
(Казань, 24 – 29 ноября 2017 г.)

Подписано в печать 21.11.2017
Бумага офсетная. Печать цифровая.
Формат 60x84 1/16. Гарнитура «Times». Усл.печ.л.10.
Тираж 200 экз. Заказ 245/11

Отпечатано с готового оригинал-макета
в типографии Издательства Казанского университета
420008, Казань, ул. Профессора Нужина, 1/37
тел. (843) 233-73-59, 233-73-28