



БЕЛОРУССКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

ЖУРНАЛ
БЕЛОРУССКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА

МАТЕМАТИКА ИНФОРМАТИКА

JOURNAL
OF THE BELARUSIAN STATE UNIVERSITY

MATHEMATICS and INFORMATICS

Издается с января 1969 г.
(до 2017 г. – под названием «Вестник БГУ.
Серия 1, Физика. Математика. Информатика»)

Выходит три раза в год

1

2020

МИНСК
БГУ

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Главный редактор **ХАРИН Ю. С.** – доктор физико-математических наук, профессор, член-корреспондент НАН Беларуси; директор Научно-исследовательского института прикладных проблем математики и информатики Белорусского государственного университета, Минск, Беларусь.
E-mail: kharin@bsu.by

**Заместители
главного редактора** **КРОТОВ В. Г.** – доктор физико-математических наук, профессор; заведующий кафедрой теории функций механико-математического факультета Белорусского государственного университета, Минск, Беларусь.
E-mail: krotov@bsu.by

ДУДИН А. Н. – доктор физико-математических наук, профессор; заведующий лабораторией прикладного вероятностного анализа факультета прикладной математики и информатики Белорусского государственного университета, Минск, Беларусь.
E-mail: dudin@bsu.by

**Ответственный
секретарь** **МАТЕЙКО О. М.** – кандидат физико-математических наук, доцент; доцент кафедры общей математики и информатики механико-математического факультета Белорусского государственного университета, Минск, Беларусь.
E-mail: matseika@bsu.by

- Абламейко С. В.** Белорусский государственный университет, Минск, Беларусь.
Альтенбах Х. Магдебургский университет им. Отто фон Герике, Магдебург, Германия.
Антоневич А. Б. Белорусский государственный университет, Минск, Беларусь.
Бауэр С. М. Санкт-Петербургский государственный университет, Санкт-Петербург, Россия.
Беняш-Кривец В. В. Белорусский государственный университет, Минск, Беларусь.
Берник В. И. Институт математики Национальной академии наук Беларуси, Минск, Беларусь.
Бухштабер В. М. Математический институт им. В. А. Стеклова Российской академии наук, Московский государственный университет им. М. В. Ломоносова, Москва, Россия.
Вабищевич П. Н. Институт проблем безопасного развития атомной энергетики Российской академии наук, Москва, Россия.
Волков В. М. Белорусский государственный университет, Минск, Беларусь.
Гладков А. Л. Белорусский государственный университет, Минск, Беларусь.
Го В. Китайский университет науки и технологий, Хэфэй, провинция Аньхой, Китай.
Гогинава У. Тбилисский государственный университет им. Иванэ Джавахишвили, Тбилиси, Грузия.
Головкин В. А. Брестский государственный технический университет, Брест, Беларусь.
Гороховик В. В. Институт математики Национальной академии наук Беларуси, Минск, Беларусь.
Громак В. И. Белорусский государственный университет, Минск, Беларусь.
Демид Г. Институт математики и информатики Вильнюсского университета, Вильнюс, Литва.
Донской В. И. Крымский федеральный университет им. В. И. Вернадского, Симферополь, Россия.
Егоров А. Д. Институт математики Национальной академии наук Беларуси, Минск, Беларусь.
Еремеев В. А. Гданьский политехнический университет, Гданьск, Польша.
Жоландек Х. Институт математики Варшавского университета, Варшава, Польша.
Журавков М. А. Белорусский государственный университет, Минск, Беларусь.
Залесский П. А. Бразильский университет, Бразилиа, Бразилия.
Зубков А. М. Московский государственный университет им. М. В. Ломоносова, Математический институт им. В. А. Стеклова Российской академии наук, Москва, Россия.
Каплунов Ю. Д. Университет Кииле, Кииле, Великобритания.
Кашин Б. С. Математический институт им. В. А. Стеклова Российской академии наук, Московский государственный университет им. М. В. Ломоносова, Москва, Россия.
Келлерер Х. Грацский университет им. Карла и Франца, Грац, Австрия.

- Княжище Л. Б.** Институт математики Национальной академии наук Беларуси, Минск, Беларусь.
- Кожанов А. И.** Институт математики им. С. Л. Соболева, Новосибирский государственный университет, Новосибирск, Россия.
- Котов В. М.** Белорусский государственный университет, Минск, Беларусь.
- Краснопрошин В. В.** Белорусский государственный университет, Минск, Беларусь.
- Лауринчикас А. П.** Вильнюсский университет, Вильнюс, Литва.
- Мадани К.** Университет Париж-Эст Марн-ла-Валле, Марн-ла-Валле, Франция.
- Макаров Е. К.** Институт математики Национальной академии наук Беларуси, Минск, Беларусь.
- Матус П. П.** Институт математики Национальной академии наук Беларуси, Минск, Беларусь.
- Медведев Д. Г.** Белорусский государственный университет, Минск, Беларусь.
- Михасев Г. И.** Белорусский государственный университет, Минск, Беларусь.
- Нестеренко Ю. В.** Московский государственный университет им. М. В. Ломоносова, Москва, Россия.
- Никоноров Ю. Г.** Южный математический институт Владикавказского научного центра Российской академии наук, Владикавказ, Россия.
- Освальд П.** Боннский университет, Бонн, Германия.
- Романовский В. Г.** Мариборский университет, Марибор, Словения.
- Рязанов В. В.** Вычислительный центр им. А. А. Дородницына Российской академии наук, Москва, Россия.
- Сафонов В. Г.** Белорусский государственный университет, Минск, Беларусь.
- Скиба А. Н.** Гомельский государственный университет им. Франциска Скорины, Гомель, Беларусь.
- Сотсков Ю. Н.** Объединенный институт проблем информатики Национальной академии наук Беларуси, Минск, Беларусь.
- Трофимов В. А.** Московский государственный университет им. М. В. Ломоносова, Москва, Россия.
- Тузиков А. В.** Объединенный институт проблем информатики Национальной академии наук Беларуси, Минск, Беларусь.
- Фильцмозер П.** Венский технический университет, Вена, Австрия.
- Черноусов В. И.** Альбертский университет, Эдмонтон, Канада.
- Чижик С. А.** Национальная академия наук Беларуси, Минск, Беларусь.
- Шешок Д.** Вильнюсский технический университет им. Гедиминаса, Вильнюс, Литва.
- Шубэ А. С.** Институт математики и информатики Академии наук Республики Молдова, Кишинев, Молдова.
- Янчевский В. И.** Институт математики Национальной академии наук Беларуси, Минск, Беларусь.

EDITORIAL BOARD

Editor-in-chief	KHARIN Y. S. , doctor of science (physics and mathematics), full professor, corresponding member of the National Academy of Sciences of Belarus; director of the Research Institute for Applied Problems of Mathematics and Informatics, Belarusian State University, Minsk, Belarus. E-mail: kharin@bsu.by
Deputy editors-in-chief	KROTOV V. G. , doctor of science (physics and mathematics), full professor; head of the department of function theory, faculty of mechanics and mathematics, Belarusian State University, Minsk, Belarus. E-mail: krotov@bsu.by
	DUDIN A. N. , doctor of science (physics and mathematics), full professor; head of the laboratory of applied probabilistic analysis, faculty of applied mathematics and computer science, Belarusian State University, Minsk, Belarus. E-mail: dudin@bsu.by
Executive secretary	MATEIKO O. M. , PhD (physics and mathematics), docent; associate professor at the department of general mathematics and computer science, faculty of mechanics and mathematics, Belarusian State University, Minsk, Belarus. E-mail: matseika@bsu.by
Ablameyko S. V.	Belarusian State University, Minsk, Belarus.
Altenbach H.	Otto-von-Guericke University, Magdeburg, Germany.
Antonevich A. B.	Belarusian State University, Minsk, Belarus.
Bauer S. M.	Saint Petersburg State University, Saint Petersburg, Russia.
Beniash-Kryvets V. V.	Belarusian State University, Minsk, Belarus.
Bernik V. I.	Institute of Mathematics of the National Academy of Sciences of Belarus, Minsk, Belarus.
Buchstaber V. M.	Steklov Institute of Mathematics of Russian Academy of Sciences, Lomonosov Moscow State University, Moscow, Russia.
Vabishchevich P. N.	Institute for the Safe Development of Atomic Energy of the Russian Academy of Sciences, Moscow, Russia.
Volkov V. M.	Belarusian State University, Minsk, Belarus.
Gladkov A. L.	Belarusian State University, Minsk, Belarus.
Guo W.	University of Science and Technology of China, Hefei, Anhui, China.
Goginava U.	Ivane Javakhishvili Tbilisi State University, Tbilisi, Georgia.
Golovko V. A.	Brest State Technical University, Brest, Belarus.
Gorokhovik V. V.	Institute of Mathematics of the National Academy of Sciences of Belarus, Minsk, Belarus.
Gromak V. I.	Belarusian State University, Minsk, Belarus.
Dzemyda G.	Institute of Mathematics and Informatics of the Vilnius University, Vilnius, Lithuania.
Donskoy V. I.	V. I. Vernadsky Crimean Federal University, Simferopol, Russia.
Egorov A. D.	Institute of Mathematics of the National Academy of Sciences of Belarus, Minsk, Belarus.
Eremeyev V. A.	Gdansk University of Technology, Gdansk, Poland.
Zoladek H.	Mathematics Institute of the University of Warsaw, Warsaw, Poland.
Zhuravkov M. A.	Belarusian State University, Minsk, Belarus.
Zalesskii P. A.	University of Brazilia, Brazilia, Brazil.
Zubkov A. M.	Lomonosov Moscow State University, Mathematical Institute of the Russian Academy of Sciences, Moscow, Russia.
Kaplunov J. D.	Keele University, Keele, United Kingdom.
Kashin B. S.	Steklov Institute of Mathematics of Russian Academy of Sciences, Lomonosov Moscow State University, Moscow, Russia.
Kellerer H.	University of Graz, Graz, Austria.
Knyazhishche L. B.	Institute of Mathematics of the National Academy of Sciences of Belarus, Minsk, Belarus.
Kozhanov A. I.	Sobolev Institute of Mathematics, Novosibirsk State University, Novosibirsk, Russia.
Kotov V. M.	Belarusian State University, Minsk, Belarus.

- Krasnoproshin V. V.** Belarusian State University, Minsk, Belarus.
- Laurinchikas A. P.** Vilnius University, Vilnius, Lithuania.
- Madani K.** Université Paris-Est, Marne-la-Vallée, France.
- Makarov E. K.** Institute of Mathematics of the National Academy of Sciences of Belarus, Minsk, Belarus.
- Matus P. P.** Institute of Mathematics of the National Academy of Sciences of Belarus, Minsk, Belarus.
- Medvedev D. G.** Belarusian State University, Minsk, Belarus.
- Mikhasev G. I.** Belarusian State University, Minsk, Belarus.
- Nesterenko Y. V.** Lomonosov Moscow State University, Moscow, Russia.
- Nikonorov Y. G.** Southern Mathematical Institute of the Vladikavkaz Scientific Center of the Russian Academy of Sciences, Vladikavkaz, Russia.
- Oswald P.** University of Bonn, Bonn, Germany.
- Romanovskij V. G.** University of Maribor, Maribor, Slovenia.
- Ryazanov V. V.** Dorodnicyn Computing Centre of the Russian Academy of Sciences, Moscow, Russia.
- Safonov V. G.** Belarusian State University, Minsk, Belarus.
- Skiba A. N.** Francisk Skorina Gomel State University, Gomel, Belarus.
- Sotskov Y. N.** United Institute of Informatics Problems of the National Academy of Sciences of Belarus, Minsk, Belarus.
- Trofimov V. A.** Lomonosov Moscow State University, Moscow, Russia.
- Tuzikov A. V.** Research Institute for Applied Problems of Mathematics and Informatics of the National Academy of Sciences of Belarus, Minsk, Belarus.
- Filzmoser P.** Vienna University of Technology, Vienna, Austria.
- Chernousov V. I.** University of Alberta, Edmonton, Canada.
- Chizhik S. A.** National Academy of Sciences of Belarus, Minsk, Belarus.
- Šešok D.** Vilnius Gediminas Technical University, Vilnius, Lithuania.
- Suba A. S.** Institute of Mathematics and Computer Science of the Academy of Sciences of Moldova, Kishinev, Moldova.
- Yanchevskii V. I.** Institute of Mathematics of the National Academy of Sciences of Belarus, Minsk, Belarus.

Вещественный, комплексный и функциональный анализ

REAL, COMPLEX AND FUNCTIONAL ANALYSIS

УДК 517.5

ВЛОЖЕНИЕ КЛАССА ХАЙЛАША – СОБОЛЕВА $M_{\alpha}^p(X)$ В ПРОСТРАНСТВО НЕПРЕРЫВНЫХ ФУНКЦИЙ В КРИТИЧЕСКОМ СЛУЧАЕ

С. А. БОНДАРЕВ¹⁾

¹⁾Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь

Пусть (X, d, μ) – метрическое пространство с мерой, удовлетворяющей условию удвоения с показателем γ , т. е. для любых шаров $B(x, R)$ и $B(x, r)$, $r < R$, выполняется неравенство

$$\mu(B(x, R)) \leq a_{\mu} \left(\frac{R}{r} \right)^{\gamma} \mu(B(x, r))$$

для некоторых положительных постоянных γ и a_{μ} . На такой общей структуре можно ввести пространство Хайлаша – Соболева $M_{\alpha}^p(X)$, которое в евклидовом случае совпадает с классическим соболевским пространством при $p > 1$, $\alpha = 1$. В статье обсуждается вложение функций из пространств Хайлаша – Соболева $M_{\alpha}^p(X)$ в пространство непрерывных функций при $p \leq 1$ в критическом случае $\gamma = \alpha p$. Более точно, показано, что любая функция из класса Хайлаша – Соболева $M_{\alpha}^p(X)$, $0 < p \leq 1$, $\alpha > 0$, имеет непрерывного представителя в случае равномерно совершенного пространства (X, d, μ) .

Ключевые слова: анализ на метрических пространствах с мерой; пространства Соболева.

Образец цитирования:

Бондарев С.А. Вложение класса Хайлаша – Соболева $M_{\alpha}^p(X)$ в пространство непрерывных функций в критическом случае. *Журнал Белорусского государственного университета. Математика. Информатика.* 2020;1:6–12 (на англ.).
<https://doi.org/10.33581/2520-6508-2020-1-6-12>

For citation:

Bondarev S.A. Inclusion of Hajlasz – Sobolev class $M_{\alpha}^p(X)$ into the space of continuous functions in the critical case. *Journal of the Belarusian State University. Mathematics and Informatics.* 2020;1:6–12.
<https://doi.org/10.33581/2520-6508-2020-1-6-12>

Автор:

Сергей Александрович Бондарев – аспирант кафедры теории функций механико-математического факультета. Научный руководитель – доктор физико-математических наук, профессор В. Г. Кротов.

Author:

Sergey A. Bondarev, postgraduate student at the department of function theory, faculty of mathematics and mechanics.
bsa0393@gmail.com

INCLUSION OF HAJŁASZ – SOBOLEV CLASS $M_\alpha^p(X)$ INTO THE SPACE OF CONTINUOUS FUNCTIONS IN THE CRITICAL CASE

S. A. BONDAREV^a

^aBelarusian State University, 4 Niezaliežnasci Avenue, Minsk 220030, Belarus

Let (X, d, μ) be a doubling metric measure space with doubling dimension γ , i. e. for any balls $B(x, R)$ and $B(x, r)$, $r < R$, following inequality holds

$$\mu(B(x, R)) \leq a_\mu \left(\frac{R}{r}\right)^\gamma \mu(B(x, r))$$

for some positive constants γ and a_μ . Hajłasz – Sobolev space $M_\alpha^p(X)$ can be defined upon such general structure. In the Euclidean case Hajłasz – Sobolev space coincides with classical Sobolev space when $p > 1$, $\alpha = 1$. In this article we discuss inclusion of functions from Hajłasz – Sobolev space $M_\alpha^p(X)$ into the space of continuous functions for $p \leq 1$ in the critical case $\gamma = \alpha p$. More precisely, it is shown that any function from Hajłasz – Sobolev class $M_\alpha^p(X)$, $0 < p \leq 1$, $\alpha > 0$, has a continuous representative in case of uniformly perfect space (X, d, μ) .

Keywords: analysis on metric measure spaces; Sobolev spaces.

Introduction

Denote by W_k^p usual Sobolev space ($p \geq 1$ is a summability parameter, $k \in \mathbb{N}$ is a smoothness parameter). These spaces were introduced by S. L. Sobolev in 1930s. They play crucial role in many areas of mathematics and applications, especially in partial differential equations. Such a big variety of applications is due to the fact that Sobolev spaces allow to define the smoothness of functions in a form suitable for literally any purpose (e. g., weak solutions of many partial differential equations exist in Sobolev spaces). Different generalizations of classical W_k^p space (say, fractional scales of these classes) play the same role. One of the possible generalizations is a Hajłasz – Sobolev class $M_\alpha^p(X)$ which allows us to define Sobolev space on arbitrary metric space X .

Nowadays there is a big interest in so called nonsmooth calculus (see [1]) due to the recent developments in fractals, nonlinear harmonic analysis, analysis on Riemannian manifolds, etc. Many facts of classical analysis can be obtained without strong assumptions on the structure of the underlying space. For example, maximal function, differentiation theorems, functions of bounded mean oscillation can be defined in the context of the space of homogenous type, which will be defined below.

That's why Sobolev classes on general metric measure spaces are of big interest as well. In [2] P. Hajłasz introduced first order Sobolev class $M_1^p(X)$ on arbitrary metric measure space (X, d, μ) for $p > 1$. This approach is based on pointwise inequalities for the pair of functions (f, g)

$$|f(x) - f(y)| \leq d(x, y)(g(x) + g(y)) \quad (1)$$

and can be considered as a Lipschitz type characterization of Sobolev functions. One can define Hajłasz – Sobolev space $M_1^p(X)$ as

$$M_1^p(X) = \{f \in L^p(X) : \exists g \in L^p(X) \text{ such that (1) holds a. e.}\}.$$

In [2] it was shown that $M_1^p(\mathbb{R}^n) = W_1^p(\mathbb{R}^n)$ for $p > 1$. D. Yang [3] introduced fractional scales of Hajłasz – Sobolev spaces $M_\alpha^p(X)$, $\alpha > 0$.

Let $\alpha, p > 0$. Hajłasz – Sobolev class $M_\alpha^p(X)$ on the metric space X consists of the functions (equivalent classes of functions) $f \in L^p(X)$, such that there exists a nonnegative function $g \in L^p(X)$ and the following inequality

$$|f(x) - f(y)| \leq (d(x, y))^\alpha (g(x) + g(y)) \quad (2)$$

takes place almost everywhere. The inequality (2) can be interpreted as a Lipschitz type characterization of Sobolev functions. Any function g which satisfies (2) is called an α -gradient of f . By $D_\alpha[f]$ we denote the set of all α -gradients. In euclidean case $X = \mathbb{R}^n$ one can take maximal function of a gradient $|\nabla f|$ as g .

One can endow space $M_\alpha^p(X)$ with norm (quasinorm for $p < 1$)

$$\|f\|_{M_\alpha^p(X)} = \|f\|_{L^p(X)} + \inf \left\{ \|g\|_{L^p(X)} \right\},$$

where infimum is taken over all $g \in L^p(X)$ that satisfy condition (2).

It is well known that functions from Sobolev space $W_1^1[0, 1]$ are absolutely continuous. What can one say about this in case of arbitrary metric space? It appears that in critical case (i. e. p is equal to the dimension of the space) any function $f \in M_1^p(X)$, $p \leq 1$, has a continuous representative if (X, d, μ) is Ahlfors regular space (see precise definition in the next section). This result was proved by X. Zhou in [4]. The goal of this paper is to generalize this result to Hajłasz – Sobolev spaces $M_\alpha^p(X)$, $\alpha > 0$, and to relax a little bit assumptions on the underlying space: one can obtain the same inclusion with uniformly perfect metric measure space satisfying doubling condition (see precise definitions in the next section). Author came to these questions while investigating Lebesgue points of functions from Hajłasz – Sobolev spaces (see [5] and [6] for subcritical and critical case respectively).

The main result of paper [4] is the following theorem.

Theorem 1. *Let $0 < p \leq 1$. Any function $f \in M_1^p(X)$ for p -Ahlfors regular metric measure space (X, d, μ) has a uniformly continuous representative. Moreover, there exists a constant c such that for any ball B and any 1-gradient $g \in D_1[f] \cap L^p(X)$*

$$\sup_{x, y \in B} |f(x) - f(y)| \leq c \left(\int_{2B} g^p d\mu \right)^{\frac{1}{p}}.$$

Re-examination of the proof of theorem 1 allows us to state a bit stronger result.

Theorem 2. *Let (X, d, μ) be a uniformly perfect metric measure space which satisfies doubling condition with doubling dimension γ . Let also $\gamma = \alpha p$, $\alpha > 0$ and $0 < p \leq 1$. Then any function $f \in M_\alpha^p(X)$ has a continuous representative. Moreover, there exists a constant c such that for any ball B and any α -gradient $g \in D_\alpha[f] \cap L^p(X)$*

$$\sup_{x, y \in B} |f(x) - f(y)| \leq c r_B^\alpha \left(\frac{1}{\mu(2B)} \int_{2B} g^p d\mu \right)^{\frac{1}{p}}. \quad (3)$$

It should be noted that expression on the right hand side of (3) tends to zero a. e. according to lemma 2.

In the Euclidean case there always exists a discontinuous function in $W_1^n(B(0, e^{-1}))$ if $n \geq 2$. Indeed, one can take as an example function $\ln|\ln|x||$ which also shows that $W_1^n(X)$ is not embedded into L^∞ space. The same result is valid for Hajłasz – Sobolev spaces $M_1^p(X)$ as well, provided that (X, d, μ) is p -Ahlfors regular. Existence of discontinuous function from $M_1^p(X)$ was shown by P. Górka and A. Ślabuszewski in [7]. Just like in the classical case they observed the function

$$f(x) = \begin{cases} \log(-\log d(x, x_0)), & x \in B(x_0, e^{-1}) \setminus \{x_0\}, \\ 0, & \text{otherwise} \end{cases}$$

for some fixed point $x_0 \in X$. It can be shown that $f(x)$ gives an example of discontinuous function in $M_1^p(X)$ [7].

Preliminaries

In this section we collect all necessary definitions and preliminary results.

Let (X, d, μ) be a metric measure space equipped with metric d and σ -finite Borel measure μ . We will assume that the measure satisfies a doubling condition, i. e. for any balls $B(x, r)$ and $B(x, R)$, $R > r$, following inequality holds

$$\mu(B(x, R)) \leq a_\mu \left(\frac{R}{r} \right)^\gamma \mu(B(x, r))$$

for some nonnegative constants a_μ and γ . In order to exclude some trivial cases we will also assume that

$$0 < \mu(B) < \infty$$

for any ball B . Then (X, d, μ) is called a space of homogeneous type. Parameter γ plays the role of the dimension of the space. Further we will be working only with measures that satisfy doubling condition.

Definition 1. We will call a metric space *uniformly perfect*, if there exists some constant $0 < \lambda < 1$ such that for any $x \in X$ and any radius $r > 0$

$$B(x, r) \setminus B(x, \lambda r) \neq \emptyset.$$

Definition 2. A metric space is called a *Ahlfors γ -regular space*, if there exist positive constants c_1, c_2 such that for any ball $B(x, r)$

$$c_1 r^\gamma \leq \mu(B(x, r)) \leq c_2 r^\gamma.$$

Important examples of Ahlfors regular spaces are fractals. For example, standard middle third Cantor set, von Koch snowflake curve and Sierpinski triangle equipped with Euclidean distance and corresponding Hausdorff measure are Ahlfors γ -regular spaces with γ equal to $\frac{\log 2}{\log 3}$, $\frac{\log 4}{\log 3}$ and $\frac{\log 3}{\log 2}$ respectively (Hausdorff dimensions of these fractals).

Note that if space is Ahlfors γ -regular then it's necessarily uniformly perfect. The converse is not true.

We use following notation for integral average of function f over the ball B

$$f_B = \oint_B f d\mu = \frac{1}{\mu(B)} \int_B f d\mu.$$

Next we recall the definition of Hardy – Littlewood maximal operator Mf :

$$Mf(x) = \sup_{B \ni x} \oint_B |f| d\mu,$$

where the supremum is taken over all balls containing point x .

The following lemma shows that maximal function satisfies weak type estimate. One may find the proof in [8] for Euclidean case and in [9, chap. 2] for general metric case. Throughout the paper by c we denote some positive constant whose value is not important and can change even in the same line.

Lemma 1. Let $f \in L^1(X)$. Then

$$\mu(\{x \in X : Mf(x) > \lambda\}) \leq c \frac{\|f\|_{L^1(X)}}{\lambda}. \quad (4)$$

Note that (4) does not necessarily hold without doubling condition.

Lemma 2. Let $0 \leq g \in L^p(X)$. Denote

$$E = \left\{ x \in X : \limsup_{r \rightarrow 0} r^{\alpha p} \oint_{B(x, r)} g^p d\mu > 0 \right\}.$$

Then $\mu(E) = 0$.

Proof. It's easy to notice that

$$E \subset F = \{x \in X : Mg^p(x) = +\infty\}.$$

Indeed, if $Mg^p(x) < \infty$ for some point x then

$$\limsup_{r \rightarrow 0} r^{\alpha p} \oint_{B(x, r)} g^p d\mu \leq Mg^p(x) \lim_{r \rightarrow 0} r^{\alpha p} = 0.$$

It's enough to show that $\mu(F) = 0$. This is a simple consequence of weak type estimate from lemma 1:

$$\mu(F) = \lim_{\lambda \rightarrow +\infty} \mu(\{x \in X : Mg^p(x) > \lambda\}) \leq c \lim_{\lambda \rightarrow +\infty} \frac{\|g^p\|_{L^1(X)}}{\lambda} = 0.$$

In order to prove main theorem we'll need one more geometric lemma. The proof can be found in [4].

Lemma 3. Let X be a uniformly perfect space. Then there exists a constant c_0 such that for any ball $B(x, r)$ there exists a sequence of balls $\{B_i\}_{i=1}^\infty = \{B(x_i, c_0^i r)\}_{i=1}^\infty$ with following properties:

- 1) $B_i \subset B(x, r)$;
- 2) $B_i \cap B_j = \emptyset, i \neq j$;
- 3) $B_i \subset B(x, c_0^{i-1}r) \setminus B(x, c_0^i r)$.

Proof of the main theorem

We will follow the ideas from [4].

Proof of theorem 2. Let $f \in M_\alpha^p(X)$. By definition there exists set $E \subset X, \mu(E) = 0$ such that inequality

$$|f(x) - f(y)| \leq (d(x, y))^\alpha (g(x) + g(y))$$

holds for any $x, y \in X \setminus E$. Denote also

$$F = \left\{ x \in X \setminus E : g(x) < \infty \text{ and } \limsup_{r \rightarrow +0} r^{\alpha p} \oint_{B(x, r)} g^p d\mu = 0 \right\}.$$

Clearly, $\mu(X \setminus F) = 0$.

Now fix the ball $B = B(z, r) \subset X$. We will show that

$$\sup_{x, y \in B \cap F} |f(x) - f(y)| \leq cr^\alpha \left(\oint_{B(z, 2r)} g^p d\mu \right)^{\frac{1}{p}}.$$

Let $x, y \in B(z, r) \cap F$. By lemma 3 there exists a sequence of balls $B_i = B(x_i, c_0^i r) \subset B(x, r)$ such that

$$B_i \subset B(x, c_0^{i-1}r) \setminus B(x, c_0^i r).$$

It's easy to see that for any $i \in \mathbb{N}$ there exists a point $z_i \in B_i \cap F$ for which

$$g(z_i) \leq \left(\oint_{B_i} g^p d\mu \right)^{\frac{1}{p}}.$$

Hence we get the chain of inequalities

$$|f(x) - f(z_i)| \leq (d(x, z_i))^\alpha (g(x) + g(z_i)) \leq cr_i^\alpha \left(g(x) + \left(\oint_{B_i} g^p d\mu \right)^{\frac{1}{p}} \right).$$

The last inequality together with lemma 2 show that

$$\lim_{i \rightarrow \infty} f(z_i) = f(x).$$

Therefore, we have

$$\begin{aligned} |f(z_1) - f(x)| &\leq \sum_{i=1}^{\infty} |f(z_i) - f(z_{i+1})| \leq \sum_{i=1}^{\infty} (d(z_i, z_{i+1}))^\alpha (g(z_i) + g(z_{i+1})) \leq \\ &\leq c \sum_{i=1}^{\infty} r_i^\alpha \left(\left(\oint_{B_i} g^p d\mu \right)^{\frac{1}{p}} + \left(\oint_{B_{i+1}} g^p d\mu \right)^{\frac{1}{p}} \right) \leq c \sum_{i=1}^{\infty} r_i^\alpha \left(\oint_{B_i} g^p d\mu \right)^{\frac{1}{p}}. \end{aligned}$$

Now, applying doubling condition and an elementary inequality

$$\sum_i a_i^{\frac{1}{p}} \leq \left(\sum_i a_i \right)^{\frac{1}{p}},$$

which holds for $0 < p \leq 1$, one can obtain

$$\begin{aligned} |f(z_1) - f(x)| &\leq c \sum_{i=1}^{\infty} r_i^{\alpha} \left(\oint_{B_i} g^p d\mu \right)^{\frac{1}{p}} = c \sum_{i=1}^{\infty} r_i^{\alpha} \left(\frac{\mu(B)}{\mu(B_i)} \frac{1}{\mu(B)} \int_{B_i} g^p d\mu \right)^{\frac{1}{p}} \leq \\ &\leq cr^{\alpha} \sum_{i=1}^{\infty} \left(\frac{1}{\mu(B)} \int_{B_i} g^p d\mu \right)^{\frac{1}{p}} \leq cr^{\alpha} \left(\frac{1}{\mu(B)} \sum_{i=1}^{\infty} \int_{B_i} g^p d\mu \right)^{\frac{1}{p}} \leq cr^{\alpha} \left(\oint_{B(z, 2r)} g^p d\mu \right)^{\frac{1}{p}}. \end{aligned} \quad (5)$$

Next inequality follows from the doubling condition and the inclusion $B_1 \subset B(z, 2r)$

$$g(z_1) \leq \left(\oint_{B_1} g^p d\mu \right)^{\frac{1}{p}} = \left(\frac{1}{\mu(2B)} \frac{\mu(2B)}{\mu(B_1)} \int_{B_1} g^p d\mu \right)^{\frac{1}{p}} \leq c \left(\oint_{2B} g^p d\mu \right)^{\frac{1}{p}}.$$

Similarly, one can find a point $w_1 \in B(y, r) \subset B(z, 2r)$ such that

$$|f(w_1) - f(x)| \leq cr^{\alpha} \left(\oint_{B(z, 2r)} g^p d\mu \right)^{\frac{1}{p}} \quad (6)$$

and

$$g(w_1) \leq c \left(\oint_{B(z, 2r)} g^p d\mu \right)^{\frac{1}{p}}.$$

It allows us to conclude that

$$g(z_1) + g(w_1) \leq c \left(\oint_{B(z, 2r)} g^p d\mu \right)^{\frac{1}{p}}.$$

Finally, in order to get inequality (3), write down triangle inequality

$$|f(x) - f(y)| \leq |f(x) - f(z_1)| + |f(z_1) - f(w_1)| + |f(w_1) - f(y)|,$$

and estimate first and third terms with help of (5) and (6) respectively. Then use the following inequality for the second term

$$|f(z_1) - f(w_1)| \leq c(d(x, y))^{\alpha} (g(z_1) + g(w_1)) \leq cr^{\alpha} \left(\oint_{B(z, 2r)} g^p d\mu \right)^{\frac{1}{p}}.$$

Taking supremum we get

$$\sup_{x, y \in B \cap F} |f(x) - f(y)| \leq cr^{\alpha} \left(\oint_{B(z, 2r)} g^p d\mu \right)^{\frac{1}{p}}.$$

Now continuity follows from lemma 2. This completes the proof of theorem 2.

Библиографические ссылки

1. Heinonen J. Nonsmooth calculus. *Bulletin of the American mathematical society*. 2007;44(2):163–232. DOI: 10.1090/s0273-0979-07-01140-8.
2. Hajlasz P. Sobolev spaces on an arbitrary metric space. *Potential Analysis*. 1996;5(4):403–415. DOI: 10.1007/BF00275475.
3. Yang D. New characterization of Hajlasz – Sobolev spaces on metric spaces. *Science in China. Series A. Mathematics*. 2003;46(5):675–689. DOI: 10.1360/02ys0343.
4. Zhou X. Sobolev functions in the critical case are uniformly continuous in s -Ahlfors regular metric spaces when $s \leq 1$. *Proceedings of the American Mathematical Society*. 2017;145:267–272. DOI: 10.1090/proc/13220.

5. Bondarev SA, Krotov VG. Fine properties of functions from Hajłasz – Sobolev classes M_α^p , $p > 0$. I. Lebesgue points. *Journal of Contemporary Mathematical Analysis*. 2016;51(6):282–295. DOI: 10.3103/S1068362316060029.
6. Бондарев СА. Точки Лебега для функций из обобщенных классов Соболева $M_\alpha^p(X)$ в критическом случае. *Журнал Белорусского государственного университета. Математика. Информатика*. 2018;3:4–11.
7. Górká P, Ślabuszeński A. A discontinuous Sobolev function exists. *Proceedings of the American Mathematical Society*. 2019; 147(2):637–639. DOI: 10.1090/proc/14164.
8. Стейн И. Сингулярные интегралы и дифференциальные свойства функций. Буренков ВИ, редактор. Москва: Мир; 1973. 342 с.
9. Heinonen J. *Lectures on analysis on metric spaces*. New York: Springer – Verlag; 2001. 141 p. (Universitext). DOI: 10.1007/978-1-4613-0131-8.

References

1. Heinonen J. Nonsmooth calculus. *Bulletin of the American mathematical society*. 2007;44(2):163–232. DOI: 10.1090/s0273-0979-07-01140-8.
2. Hajłasz P. Sobolev spaces on an arbitrary metric space. *Potential Analysis*. 1996;5(4):403–415. DOI: 10.1007/BF00275475.
3. Yang D. New characterization of Hajłasz – Sobolev spaces on metric spaces. *Science in China. Series A. Mathematics*. 2003; 46(5):675–689. DOI: 10.1360/02ys0343.
4. Zhou X. Sobolev functions in the critical case are uniformly continuous in s -Ahlfors regular metric spaces when $s \leq 1$. *Proceedings of the American Mathematical Society*. 2017;145:267–272. DOI: 10.1090/proc/13220.
5. Bondarev SA, Krotov VG. Fine properties of functions from Hajłasz – Sobolev classes M_α^p , $p > 0$. I. Lebesgue points. *Journal of Contemporary Mathematical Analysis*. 2016;51(6):282–295. DOI: 10.3103/S1068362316060029.
6. Bondarev SA. Lebesgue points of functions from generalized Sobolev classes $M_\alpha^p(X)$ in the critical case. *Journal of the Belarusian State University. Mathematics and Informatics*. 2018;3:4–11. Russian.
7. Górká P, Ślabuszeński A. A discontinuous Sobolev function exists. *Proceedings of the American Mathematical Society*. 2019; 147(2):637–639. DOI: 10.1090/proc/14164.
8. Stein E. *Singular integrals and differentiability properties of functions*. Princeton: Princeton University Press; 1970. 287 p. Russian edition: Stein E. *Singulyarnye integraly i differentsial'nye svoistva funktsii*. Burenkov VI, editor. Moscow: Mir; 1973. 342 p.
9. Heinonen J. *Lectures on analysis on metric spaces*. New York: Springer – Verlag; 2001. 141 p. (Universitext). DOI: 10.1007/978-1-4613-0131-8.

Received by editorial board 22.01.2020.

МАТЕМАТИЧЕСКАЯ ЛОГИКА, АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

MATHEMATICAL LOGIC, ALGEBRA AND NUMBER THEORY

УДК 511.235+519.719.2

АНАЛИЗ RSA-КРИПТОСИСТЕМЫ В АБСТРАКТНЫХ ЧИСЛОВЫХ КОЛЬЦАХ

Н. В. КОНДРАТЁНОК¹⁾

¹⁾Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь

Квантовые компьютеры могут представлять реальную угрозу для некоторых современных криптосистем, например таких, как RSA-криптосистема. Аналог последней в абстрактных числовых кольцах не подвержен этой угрозе, так как в настоящий момент нет алгоритмов факторизации идеалов, использующих квантовые вычисления. В настоящей работе исследована RSA-криптосистема в абстрактных числовых кольцах, доказаны аналоги теорем, связанных с ее криптостойкостью. В частности, доказан аналог теоремы Винера о малой секретной экспоненте. Изучен метод, аналогичный методу повторного шифрования, и на его основе получены необходимые ограничения на параметры криптосистемы. Также показано, что в числовых дедекиндовых кольцах задача факторизации полиномиально эквивалентна факторизации в целых числах.

Ключевые слова: RSA-криптосистема; абстрактное числовое кольцо; дедекиндово кольцо; факторизация; идеал.

Благодарность. Автор признателен за полезные замечания по данной статье своему научному руководителю – кандидату физико-математических наук М. М. Васьковскому.

Образец цитирования:

Кондратёнок НВ. Анализ RSA-криптосистемы в абстрактных числовых кольцах. *Журнал Белорусского государственного университета. Математика. Информатика.* 2020;1: 13–21.

<https://doi.org/10.33581/2520-6508-2020-1-13-21>

For citation:

Kondratyionok NV. Analysis of the RSA-cryptosystem in abstract number rings. *Journal of the Belarusian State University. Mathematics and Informatics.* 2020;1:13–21. Russian. <https://doi.org/10.33581/2520-6508-2020-1-13-21>

Автор:

Никита Васильевич Кондратёнок – магистрант факультета прикладной математики и информатики. Научный руководитель – кандидат физико-математических наук М. М. Васьковский.

Author:

Nikita V. Kondratyionok, master's degree student at the faculty of applied mathematics and computer science. nkondr2006@rambler.ru
<https://orcid.org/0000-0002-6109-5635>



ANALYSIS OF THE RSA-CRYPTOSYSTEM IN ABSTRACT NUMBER RINGS

N. V. KONDRATYONOK^a

^aBelarusian State University, 4 Niezaliežnasci Avenue, Minsk 220030, Belarus

Quantum computers can be a real threat to some modern cryptosystems (such as the RSA-cryptosystem). The analogue of the RSA-cryptosystem in abstract number rings is not affected by this threat, as there are currently no factorization algorithms using quantum computing for ideals. In this paper considered an analogue of RSA-cryptosystem in abstract number rings. Proved the analogues of theorems related to its cryptographic strength. In particular, an analogue of Wiener's theorem on the small secret exponent is proved. The analogue of the re-encryption method is studied. On its basis the necessary restrictions on the parameters of the cryptosystem are obtained. It is also shown that in numerical Dedekind rings the factorization problem is polynomial equivalent to factorization in integers.

Keywords: RSA-cryptosystem; abstract number ring; Dedekind ring; factorization; ideal.

Acknowledgements. I thank my supervisor PhD (physics and mathematics) M. M. Vas'kovskii for reading the work and comments.

Введение

Впервые криптосистема RSA была предложена Р. Ривестом, А. Шамиром и Л. Адлеманом в августе 1977 г. Полное ее описание опубликовано в журнале «Communications of the ACM» в феврале 1978 г. [1]. Алгоритм был основан на вычислительной сложности задачи факторизации натуральных чисел. Впоследствии сделано много обобщений этой криптосистемы. Известны ее модификации для многочленов и гауссовых чисел [2–5]. В работе [6] представлен аналог RSA-криптосистемы в квадратичных кольцах, а также доказан ряд теорем, связанных с ее безопасностью, в том числе описан способ защиты от атаки методом повторного шифрования и доказан аналог теоремы Винера о малой секретной экспоненте. В [7] RSA-криптосистема обобщена на случай произвольных абстрактных числовых колец, в качестве элементов криптосистемы предлагается брать не элементы кольца, а его идеалы. В отличие от классической RSA-криптосистемы такое обобщение неуязвимо от взлома с помощью квантовых алгоритмов факторизации, так как аналогичный алгоритм для абстрактных числовых колец пока не разработан.

Цель работы – изучение аналога RSA-криптосистемы в абстрактных числовых кольцах, а также доказательство аналогичных теорем, связанных с ее безопасностью.

Рассмотрим произвольное кольцо R . Идеалом кольца R называется подкольцо, замкнутое относительно умножения на элементы из R . Коммутативное кольцо с единицей и без делителей нуля называется *дедекиндовым*, если любой собственный идеал в нем раскладывается в конечное произведение простых идеалов. Более того, можно показать, что это разложение единственно с точностью до перестановки множителей.

Определение [8]. Абстрактное числовое кольцо – это такое дедекиндово кольцо R , что $|R/\mathfrak{m}| < \infty$ для любого ненулевого идеала $\mathfrak{m}$.

Примеры абстрактных числовых колец [8]:

- кольцо целых алгебраических чисел числового поля K ;
- кольцо координат $\mathbb{F}_q[C^\circ]$ неособой интегральной аффинной кривой $C^\circ/\mathbb{F}_q$.

Мощность множества $R/\mathfrak{m}$ называется нормой $\mathfrak{m}$ и обозначается $\mathcal{N}(\mathfrak{m})$.

Далее будем рассматривать только абстрактные числовые кольца.

В кольце R можно ввести аналог функции Эйлера $\varphi(\mathfrak{m}) = |(R/\mathfrak{m})^\times|$, где $(R/\mathfrak{m})^\times$ – группа единиц. Имеет место свойство мультипликативности:

$$\varphi\left(\prod_{i=1}^k \mathfrak{m}_i^{\alpha_i}\right) = \prod_{i=1}^k \varphi(\mathfrak{m}_i^{\alpha_i}).$$

В случае максимального идеала $\mathfrak{m}$ также выполнено следующее свойство:

$$\varphi(\mathfrak{m}^\alpha) = (\mathcal{N}(\mathfrak{m}))^\alpha - (\mathcal{N}(\mathfrak{m}))^{\alpha-1}.$$

Для введенного аналога функции Эйлера справедлива теорема Эйлера.

Утверждение 1 [7]. Пусть R – абстрактное числовое кольцо, $m \in \mathbb{R}$, $\mathfrak{U} \subset R$ – идеал. Если $Rm + \mathfrak{U} = R$, то $m^{\varphi(\mathfrak{U})} \equiv 1 \pmod{\mathfrak{U}}$.

Обозначим через $\mathcal{O}_K$ кольцо целых алгебраических чисел произвольного числового поля K . Кольцо $\mathcal{O}_K$ является абстрактным числовым кольцом. Также пусть $\mathcal{O}_K^\times$ – группа единиц кольца $\mathcal{O}_K$, $\text{Nm}(m)$ – норма элемента $m \in \mathcal{O}_K$, $\mathcal{O}_{K,m} = \mathcal{O}_K/m$ и $\mathcal{O}_{K,m}^\times$ – аддитивная и мультипликативная группа вычетов по модулю m соответственно.

Существует два способа представления идеалов [9; 10]:

- $\mathbb{Z}$ -представление: $\mathfrak{p} = \bigoplus_{i=1}^n \mathbb{Z}\alpha_i$, где $\alpha_i \in \mathcal{O}_K$;
- 2-представление: для любого $\alpha \in \mathfrak{p}$ существует $\beta \in \mathfrak{p}$ такое, что $\mathfrak{p} = \alpha\mathcal{O}_K + \beta\mathcal{O}_K$.

Будем обозначать идеалы в 2-представлении через (α, β) , порожденный элементом $\alpha \in \mathcal{O}_K$ главный идеал – через $(\alpha) = \alpha\mathcal{O}_K$.

Утверждение 2. Пусть $m \in \mathcal{O}_K$. Тогда $\mathcal{N}((m)) = |\text{Nm}(m)|$, также $(m) | (\text{Nm}(m))$.

Напомним теорему Копперсмита, которая используется ниже при доказательстве одной из теорем о безопасности криптосистемы.

Теорема Копперсмита [11]. Пусть $f(x, y)$ – неприводимый многочлен от двух переменных над $\mathbb{Z}$ со степенью δ по каждой переменной отдельно. Пусть X, Y – границы предполагаемого решения (x_0, y_0) и W – модуль максимального коэффициента $f(xY, yY)$. Если $XY \leq W^{2/(3\delta)}$, то существует полиномиальный относительно $\log W$ и 2^δ алгоритм, который позволяет найти все (x_0, y_0) такие, что $f(x_0, y_0) = 0$, $|x_0| \leq X$ и $|y_0| \leq Y$.

Теорема Дедекинда [12]. Пусть $K = \mathbb{Q}(\theta)$ – числовое поле, $f(T)$ – минимальный многочлен алгебраического числа $\theta \in \mathbb{Z}[T]$. Для простого рационального числа p , не делящего индекс $[\mathcal{O} : \mathbb{Z}[\theta]]$, запишем: $f(T) \equiv \pi_1(T)^{e_1} \cdots \pi_g(T)^{e_g} \pmod{p}$, где $\pi_i(T)$ – различные монические неприводимые многочлены в $\mathbb{F}_p[T]$, $i = \overline{1, g}$. Тогда $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$, где $\mathfrak{p}_i = (p_i, T_i(\theta))$, $T_i(T) \equiv \pi_i(T) \pmod{p}$.

Аналог RSA-криптосистемы в дедекиндовых кольцах

В работе [7] был предложен аналог RSA-криптосистемы в R и доказана его корректность. Генерация ключей этой системы происходит следующим образом:

- выбираются максимальные идеалы $\mathfrak{p}, \mathfrak{q} \subset R$;
- вычисляется значение функции Эйлера $\varphi(\mathfrak{N})$, где $\mathfrak{N} = \mathfrak{p}\mathfrak{q}$;
- выбирается целое число $e \in [1, \varphi(\mathfrak{N})]$ такое, что $(e, \varphi(\mathfrak{N})) = 1$;
- по расширенному алгоритму Евклида вычисляется число d такое, что $ed \equiv 1 \pmod{\varphi(\mathfrak{N})}$.

Пара $(\mathfrak{N}, e)$ публикуется в качестве открытого ключа RSA, а пара $(\mathfrak{N}, d)$ играет роль закрытого ключа RSA. Отображение $f : R/\mathfrak{N} \rightarrow R/\mathfrak{N}$, $f(x) \equiv x^e \pmod{\mathfrak{N}}$, называется функцией шифрования, отображение $f^{-1} : R/\mathfrak{N} \rightarrow R/\mathfrak{N}$, $f^{-1}(x) \equiv x^d \pmod{\mathfrak{N}}$, – функцией расшифрования.

Нетрудно заметить, что, зная разложение на множители $\mathfrak{N} = \mathfrak{p}\mathfrak{q}$ для RSA-модуля, можно эффективно найти секретный ключ. В [6] получено обратное утверждение для норменно-евклидовых колец. Докажем аналогичную теорему для произвольного кольца с единственной факторизацией. Далее в теоремах будем рассматривать кольцо R определенного вида, а именно кольцо $\mathcal{O}_K$ целых алгебраических чисел числового поля K . Известно, что оно дедекиндово и удовлетворяет условиям выше.

Теорема 1. Пусть $\mathcal{O}_K$ – кольцо с единственной факторизацией. В этом случае каждому идеалу соответствует некоторый элемент кольца. Пусть (N, e, d) – параметры RSA-криптосистемы в $\mathcal{O}_K$. Если d известно, то N можно эффективно разложить на множители с вероятностью не менее $\frac{1}{2}$ за полиномиальное относительно длины N количество арифметических операций в $\mathcal{O}_K$.

Доказательство. Пусть $s = ed - 1 = 2^t u$, где $t, u \in \mathbb{Z}$ и u нечетное. Так как $\varphi(N) | s$, то $x^s \equiv 1 \pmod{N}$ для всех $x \in \mathcal{O}_{K,N}^\times$. Обозначим $\mathcal{S}_N$ множество таких элементов $a \in \mathcal{O}_{K,N}^\times$, что $a^u \equiv 1 \pmod{N}$ или существует $k \in \{0, \dots, t-1\}$, при котором $a^{2^k u} \equiv -1 \pmod{N}$. Пусть $A = \mathcal{O}_{K,N}^\times \setminus \mathcal{S}_N$. Рассмотрим произвольный элемент $a \in A$ и выберем наименьшее положительное число k такое, что $a^{2^k u} \equiv 1 \pmod{N}$. Пусть

$b \equiv a^{2^{k-1}u} \pmod{N}$. Легко заметить, что $b^2 \equiv 1 \pmod{N}$ и $b \not\equiv \pm 1 \pmod{N}$. Следовательно, $(b-1, N)$ – собственный делитель N . В [13] показано, что наибольший общий делитель $(b-1, N)$ можно вычислить за полиномиальное относительно $\log Nm(N)$ число арифметических операций в $\mathcal{O}_K$. Аналогично случаю норменно-евклидовых колец можно показать, что $|\mathcal{S}_N| \leq \frac{\varphi(N)}{2}$. Доказательство завершено.

Следующая теорема является аналогом теоремы Винера о малой секретной экспоненте [14]. Таковой для квадратичного кольца с единственной факторизацией был доказан в [6].

Теорема 2. Пусть $(\mathfrak{N}, e, d)$, $\mathfrak{N} = pq$, – параметры RSA-криптосистемы в абстрактном числовом кольце R , причем выполнено соотношение $\mathcal{N}(q) < \mathcal{N}(p) < \alpha^2 \mathcal{N}(q)$, где $\alpha > 1$. Если $d < \frac{(\mathcal{N}(\mathfrak{N}))^{1/4}}{\sqrt{2\alpha+2}}$, то d можно эффективно вычислить за полиномиальное относительно $\log \mathcal{N}(\mathfrak{N})$ число бинарных операций.

Доказательство. Пусть $ed - 1 = k\varphi(\mathfrak{N})$, $k \in \mathbb{Z}$. Так как $\mathcal{N}(q) + \mathcal{N}(p) < (\alpha + 1)\sqrt{\mathcal{N}(\mathfrak{N})}$, то $\mathcal{N}(\mathfrak{N}) - \varphi(\mathfrak{N}) = \mathcal{N}(p) + \mathcal{N}(q) - 1 < (\alpha + 1)\sqrt{\mathcal{N}(\mathfrak{N})}$. Поскольку $k\varphi(\mathfrak{N}) < ed$, $e < \varphi(\mathfrak{N})$, то $k < d$. Из последнего следует неравенство

$$\frac{(\alpha + 1)k}{d\sqrt{\mathcal{N}(\mathfrak{N})}} < \frac{1}{2d^2}.$$

Принимая в расчет соотношения выше, получим

$$\left| \frac{e}{\mathcal{N}(\mathfrak{N})} - \frac{k}{d} \right| < \frac{1}{2d^2},$$

следовательно, $\frac{k}{d}$ – подходящая дробь для нескретной дроби $\frac{e}{\mathcal{N}(\mathfrak{N})}$. Таким образом, $\frac{k}{d}$ можно вычислить, используя алгоритм Евклида в $\mathbb{Z}$. Теорема доказана.

Один из известных способов взлома RSA-криптосистемы – это метод повторного шифрования. Пусть $(\mathfrak{N}, e, d)$ – параметры RSA-криптосистемы, $y \equiv x^e \pmod{\mathfrak{N}}$ – зашифрованное сообщение $x \in \mathcal{O}_{K, \mathfrak{N}}$. Для нахождения x вычисляем элементы последовательности $y_i = y^{e^i} \pmod{\mathfrak{N}}$, $i = 1, 2, \dots$, пока не получим $y_m = y$. Несложно показать, что $y_{m-1} = x$. Итак, параметры RSA-криптосистемы надо выбирать таким образом, чтобы m было достаточно велико.

Следующая теорема дает ответ на вопрос о безопасности RSA-криптосистемы относительно атаки повторным шифрованием. Ее доказательство аналогично доказательству теоремы из [6] для случая квадратичных колец с единственной факторизацией.

Теорема 3. Пусть $\mathfrak{N} = pq$ – модуль RSA-криптосистемы в кольце $\mathcal{O}_K$. Предположим, существуют различные простые числа r, s и положительные целые k, l такие, что $\varphi(p) = rk$, $\varphi(q) = sl$, и $r-1, s-1$ имеют разные простые делители r_1, s_1 соответственно. Пусть y и e – независимые равномерно распределенные случайные величины со значениями в $\mathcal{O}_{K, \mathfrak{N}}$ и $\mathbb{Z}_{\varphi(\mathfrak{N})}^*$ соответственно. Тогда для вероятности выполняется неравенство

$$\mathbb{P}(m_{e,y} \geq r_1 s_1) \geq (1 - r^{-1})(1 - s^{-1})(1 - r_1^{-1})(1 - s_1^{-1}),$$

где $m_{e,y}$ – наименьшее натуральное число такое, что $y^{e^{m_{e,y}}} \equiv y \pmod{\mathfrak{N}}$.

Доказательство. Оценим вероятность $\mathbb{P}\{rs \mid \text{ord}_{\mathcal{O}_{K, \mathfrak{N}}}^\times(y)\}$. Так как $\mathcal{O}_{K, \mathfrak{N}}^\times \cong \mathcal{O}_{K, p}^\times \times \mathcal{O}_{K, q}^\times$ и группы $\mathcal{O}_{K, p}^\times, \mathcal{O}_{K, q}^\times$ циклические, то можно записать $y = (a^i, b^j)$, где a и b – примитивные элементы $\mathcal{O}_{K, p}^\times$ и $\mathcal{O}_{K, q}^\times$ соответственно; i и j – случайные величины со значениями из $\{1, \dots, rk\}$ и $\{1, \dots, sl\}$ соответственно. Легко заметить, что

$$\text{ord}_{\mathcal{O}_{K, \mathfrak{N}}}^\times(y) = \text{lcm}\left(\frac{rk}{(rk, i)}, \frac{sl}{(sl, j)}\right).$$

Если $r \nmid i$ и $s \nmid j$, то $\text{ord}_{\mathcal{O}_{K,\mathfrak{N}}^\times}(y) \nmid rs$. Таким образом,

$$\mathbb{P}\left(rs \mid \text{ord}_{\mathcal{O}_{K,\mathfrak{N}}^\times}(y)\right) \geq \mathbb{P}\{r \nmid i, s \nmid j\} = \frac{\varphi(r)k\varphi(s)l}{rksl} = \left(1 - \frac{1}{r}\right)\left(1 - \frac{1}{s}\right).$$

Так как $e \in \mathbb{Z}_{rs}^*$, то аналогично можно получить неравенство

$$\mathbb{P}\left(r_1 s_1 \mid \text{ord}_{\mathbb{Z}_{rs}^*}(e)\right) \geq \left(1 - \frac{1}{r_1}\right)\left(1 - \frac{1}{s_1}\right).$$

Легко заметить, что $\text{ord}_{W_{\mathfrak{N}}^\times}(y) \mid (e^{m_{e,y}} - 1)$, поэтому

$$\left\{rs \mid \text{ord}_{\mathcal{O}_{K,\mathfrak{N}}^\times}(y)\right\} \subseteq \left\{\text{ord}_{\mathbb{Z}_{rs}^*}(e) \mid m_{e,y}\right\}.$$

Из приведенных выше соотношений следует, что

$$\begin{aligned} \mathbb{P}(m_{e,y} \geq r_1 s_1) &\geq \mathbb{P}(r_1 s_1 \mid m_{e,y}) \geq \mathbb{P}(r_1 s_1 \mid \text{ord}_{\mathbb{Z}_{rs}^*}(e), rs \mid \text{ord}_{\mathcal{O}_{K,\mathfrak{N}}^\times}(y)) \geq \\ &\geq (1 - r^{-1})(1 - s^{-1})(1 - r_1^{-1})(1 - s_1^{-1}). \end{aligned}$$

Теорема доказана.

Замечание 1. Для обеспечения безопасности RSA-криптосистемы в кольце с единственной факторизацией $\mathcal{O}_K$ против атаки повторного шифрования необходимо брать такие идеалы $\mathfrak{p}, \mathfrak{q} \subset \mathcal{O}_K$, для которых существуют большие различные простые делители r, s чисел $\varphi(\mathfrak{p}), \varphi(\mathfrak{q})$ и большие различные простые делители r_1, s_1 чисел $r - 1, s - 1$.

Теорема 4. Пусть $(\mathfrak{N}, e, d)$ – параметры RSA-криптосистемы в $\mathcal{O}_K$, где $\mathcal{N}(\mathfrak{p}), \mathcal{N}(\mathfrak{q})$ имеют одинаковую битовую длину. Пусть $ed \leq (\mathcal{N}(\mathfrak{N}))^2$, $\mathcal{N}(\mathfrak{N}) \geq 107$. Если d известно, то существует полиномиальный алгоритм (относительно $\log W$), который позволяет найти $\mathcal{N}(\mathfrak{p}), \mathcal{N}(\mathfrak{q})$.

Доказательство. Из $ed \equiv 1 \pmod{\varphi(\mathfrak{N})}$ следует $ed = k\varphi(\mathfrak{N}) + 1$ для некоторого $k \in \mathbb{N}$. Предположим, что $\mathcal{N}(\mathfrak{p}) \leq \mathcal{N}(\mathfrak{q})$. Тогда

$$\mathcal{N}(\mathfrak{p}) \leq (\mathcal{N}(\mathfrak{N}))^{1/2} \leq \mathcal{N}(\mathfrak{q}) < 2\mathcal{N}(\mathfrak{p}) \leq 2(\mathcal{N}(\mathfrak{N}))^{1/2}.$$

Следовательно,

$$\mathcal{N}(\mathfrak{p}) + \mathcal{N}(\mathfrak{q}) < 3(\mathcal{N}(\mathfrak{N}))^{1/2} \leq \frac{\mathcal{N}(\mathfrak{N})}{2}.$$

Из этого неравенства имеем

$$\begin{aligned} \varphi(\mathfrak{N}) &= (\mathcal{N}(\mathfrak{p}) - 1)(\mathcal{N}(\mathfrak{q}) - 1) = \mathcal{N}(\mathfrak{N}) + 1 - \mathcal{N}(\mathfrak{p}) - \mathcal{N}(\mathfrak{q}) > \\ &> \mathcal{N}(\mathfrak{N}) + 1 - \frac{\mathcal{N}(\mathfrak{N})}{2} > \frac{\mathcal{N}(\mathfrak{N})}{2}. \end{aligned}$$

Обозначим $\bar{k} = \frac{ed - 1}{\mathcal{N}(\mathfrak{N})}$. Тогда

$$k - \bar{k} = \frac{(\mathcal{N}(\mathfrak{N}) - \varphi(\mathfrak{N}))(ed - 1)}{\mathcal{N}(\mathfrak{N})\varphi(\mathfrak{N})} = \frac{(\mathcal{N}(\mathfrak{p}) + \mathcal{N}(\mathfrak{q}) - 1)(ed - 1)}{\mathcal{N}(\mathfrak{N})\varphi(\mathfrak{N})}.$$

Из выражений выше следует, что $k - \bar{k} < 6(\mathcal{N}(\mathfrak{N}))^{-3/2}(ed - 1)$.

Пусть $x = k - \bar{k}$. Также выполнено $\mathcal{N}(\mathfrak{N}) - \varphi(\mathfrak{N}) = \mathcal{N}(\mathfrak{p}) + \mathcal{N}(\mathfrak{q}) - 1 < 3(\mathcal{N}(\mathfrak{N}))^{1/2}$. Следовательно, $\varphi(\mathfrak{N}) \in \left[\mathcal{N}(\mathfrak{N}) - 3(\mathcal{N}(\mathfrak{N}))^{1/2}, \mathcal{N}(\mathfrak{N})\right]$. Разделим этот интервал на 6 интервалов длиной $\frac{(\mathcal{N}(\mathfrak{N}))^{1/2}}{2}$

с центрами в точках $\mathcal{N}(\mathfrak{N}) - \frac{2i-1}{4}(\mathcal{N}(\mathfrak{N}))^{1/2}$, $i = \overline{1, 6}$. Рассмотрим $i \in \{1, \dots, 6\}$ такое, что

$$\left|\mathcal{N}(\mathfrak{N}) - \frac{2i-1}{4}(\mathcal{N}(\mathfrak{N}))^{1/2} - \varphi(\mathfrak{N})\right| \leq \frac{1}{4}(\mathcal{N}(\mathfrak{N}))^{1/2}.$$

Пусть $g = \frac{2i-1}{4} \mathcal{N}(\mathfrak{N})$. Тогда $|\mathcal{N}(\mathfrak{N}) - g - \varphi(\mathfrak{N})| < \frac{1}{4}(\mathcal{N}(\mathfrak{N}))^{1/2} + 1$ и $\varphi(\mathfrak{N}) = \mathcal{N}(\mathfrak{N}) - g - y$ для некоторого неизвестного y такого, что $|y| \leq \frac{1}{4}(\mathcal{N}(\mathfrak{N}))^{1/2}$. Далее получим

$$ed - 1 = k\varphi(\mathfrak{N}) = (\lceil \bar{k} \rceil + x)(\mathcal{N}(\mathfrak{N}) - g - y).$$

Рассмотрим многочлен

$$f(x, y) = xy - (\mathcal{N}(\mathfrak{N}) - g)x + \lceil \bar{k} \rceil y - \lceil \bar{k} \rceil (\mathcal{N}(\mathfrak{N}) - g) + ed - 1,$$

у которого есть корень $(x_0, y_0) = (k - \lceil \bar{k} \rceil, \mathcal{N}(\mathfrak{p}) + \mathcal{N}(\mathfrak{q}) + 1 - g)$. Имеем $\delta = 1$, где δ из теоремы Копперсмита. Положим $X = 6(\mathcal{N}(\mathfrak{N}))^{1/2}$, $Y = \frac{1}{4}(\mathcal{N}(\mathfrak{N}))^{1/2} + 1$. Тогда $|x_0| \leq X$ и $|y_0| \leq Y$. Пусть W – норма вектора коэффициентов многочлена $f(xX, yY)$, для которой справедливо $W \geq (\mathcal{N}(\mathfrak{N}) - g)X > 3(\mathcal{N}(\mathfrak{N}))^{3/2}$. Следовательно,

$$XY = \frac{3}{2}\mathcal{N}(\mathfrak{N}) + 6(\mathcal{N}(\mathfrak{N}))^{1/2} < W^{2/3} = W^{2/(3\delta)}$$

для $\mathcal{N}(\mathfrak{N}) \geq 107$.

Теперь можно применить теорему Копперсмита и найти корень (x_0, y_0) за полиномиальное относительно $\log W$ время. Данный корень позволяет определить $\mathcal{N}(\mathfrak{p})$, $\mathcal{N}(\mathfrak{q})$. Теорема доказана.

Заметим, что теорема 4 – это аналог известного результата для RSA-криптосистемы в целых числах [15]. Еще одним ограничением на выбор RSA-ключей является то, что RSA-модули должны быть различными для разных пользователей. Покажем, что при реализации аналога RSA-криптосистемы это ограничение сохраняется в определенных кольцах.

Обозначим $\Lambda_K = \sup_{m/n \in F} \left| \frac{m}{n} \right|$, где $\left| \frac{m}{n} \right| = \frac{v(m)}{v(n)}$ для $\frac{m}{n} \in F \setminus \{0\}$, $|0| = 0$, F – множество правильных несо-

кратимых дробей поля частных K , $v(m)$ – норма в кольце K .

Теорема 5. Пусть $\mathbb{K}$ – евклидово кольцо относительно нормы $v(\cdot)$, $\Lambda_{\mathbb{K}} < 1$, и кольцо вычетов любого элемента $\mathbb{K}$ конечно. Тогда в $\mathbb{K}$ можно рассмотреть реализацию RSA-криптосистемы. Предположим, что два пользователя имеют одинаковые RSA-модули, но разные секретные экспоненты e_1 и e_2 , $(e_1, e_2) = 1$. Пусть перехвачены сообщения $c_1 \equiv m^{e_1} \pmod{N}$ и $c_2 \equiv m^{e_2} \pmod{N}$, где $c_1, c_2, m, N \in \mathbb{K}$. Тогда сообщение m можно вычислить за полиномиальное относительно $\log v(N)$ количество арифметических операций в $\mathbb{K}$.

Доказательство. Условие $(e_1, e_2) = 1$ означает, что существуют $s_1, s_2 \in \mathbb{Z}$ такие, что $e_1 s_1 + e_2 s_2 = 1$. Следовательно, можно вычислить

$$c_1^{s_1} c_2^{s_2} = (m^{e_1})^{s_1} (m^{e_2})^{s_2} = m^{e_1 s_1 + e_2 s_2} = m.$$

Единственная сложность заключается в том, что одно из чисел s_1, s_2 будет отрицательным. Не нарушая общности, предположим, что $s_2 < 0$. Тогда можно записать $c_2^{s_2} = (c_2^{-1})^{|s_2|}$. Требуется найти $c_2^{-1} \pmod{N}$, что эквивалентно решению уравнения $c_2 x + Ny = (c_2, N)$. Если $(c_2, N) \neq 1$, то известно разложение N на простые множители и сообщение m можно вычислить стандартным способом. В случае $(c_2, N) = 1$ надо решить уравнение $c_2 x + Ny = 1$, что можно сделать с помощью цепочек деления. Из теоремы 2 в работе [16] следует, что $l_n(\mathbb{K}) \leq \left\lceil \log_{\Lambda_{\mathbb{K}}^{-1}} n \right\rceil + 2$. Это означает, что длина цепочки с выбором минимального по норме остатка для c_2 и N ограничена логарифмом от их модуля. Следовательно, ее можно найти за полиномиальное относительно $\log v(N)$ количество арифметических операций в $\mathbb{K}$. Из построения RSA-криптосистемы следует, что $e_1 < v(N)$ и $e_2 < v(N)$, поэтому сообщение m можно вычислить за полиномиальное относительно $\log v(N)$ количество арифметических операций в $\mathbb{K}$. Теорема доказана.

Замечание 2. В [17] показано, что $\Lambda_{\mathbb{K}} < 1$ во всех квадратичных норменно-евклидовых кольцах.

Субэкспоненциальные алгоритмы факторизации в числовых полях

Приведем способ разложения идеала на произведение простых идеалов и таким образом покажем, что задача факторизации идеалов эквивалентна задаче факторизации целых чисел. Данная проблема актуальна и была рассмотрена в [18], где приведен алгоритм по определению степени простого идеала в разложении другого идеала. В настоящей работе строится алгоритм нахождения простых идеалов из разложения идеала и их степеней.

Пусть дан идеал (N) в форме своего 2-представления. Для начала запишем основные шаги алгоритма факторизации.

Шаг 1. Считаем норму идеала равной норме элемента N и раскладываем ее на множители одним из известных алгоритмов для факторизации целых чисел:

$$\text{Nm}(N) = \prod_{i=1}^k p_i^{\alpha_i}.$$

Следовательно,

$$(\text{Nm}(N)) = \prod_{i=1}^k (p_i)^{\alpha_i}.$$

Шаг 2. Факторизуем идеал (p_i) с помощью теоремы Дедекинда и получаем двухэлементные представления идеалов

$$(p_i) = \prod_{j=1}^{l_i} (p_i, f_{i,j}(\theta)).$$

Шаг 3. Преобразуем полученные простые идеалы в $\mathbb{Z}$ -представление и объединяем равные. В итоге имеем

$$(\text{Nm}(N)) = \prod_{i=1}^l \mathfrak{p}_i^{\beta_i}.$$

Шаг 4. Находим с помощью бинарного поиска степени, в которых $\mathfrak{p}_i$ входит в (N) .

Для вычисления нормы идеала (N) необходимо найти определитель матрицы, которая получается при матричном представлении элемента N . Таким образом, справедливо следующее утверждение.

Утверждение 3. Для вычисления нормы идеала (N) необходимо $O(\log^2 |N|)$ бинарных операций, где $|N|$ обозначает максимальный по модулю элемент матричного представления N .

Предположим, что $\mathcal{O}_K$ фиксировано. Значит, известны индекс $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ и разложение на простые идеалы всех простых делителей индекса. Следуя второму шагу алгоритма, рассмотрим простое число p и оценим сложность разложения идеала (p) на множители. Также оценим сложность разложения многочлена на множители в $\mathbb{F}_p$. Так как степень многочлена не превосходит константы, сделать это можно с помощью вероятностной версии алгоритма Берлекэмпса за $O(\log^3 p)$ бинарных операций. В результате разложения получим многочлены, количество которых не превосходит константы, зависящей только от $\mathcal{O}_K$. Тогда вычислить значения многочленов в разложении можно за $O(\log^2 p)$ операций. Таким образом, доказано следующее утверждение.

Утверждение 4. Разложить идеал (p) , используя теорему Дедекинда, можно за $O(\log^3 p)$ бинарных операций.

Рассмотрим преобразование идеала из 2-представления в $\mathbb{Z}$ -представление.

Утверждение 5. Преобразовать 2-представление идеала (p, α) из теоремы Дедекинда в $\mathbb{Z}$ -представление можно за $O(P(\log p))$ бинарных операций, где $P(T)$ – некоторый полином.

Доказательство. В [19] описан алгоритм преобразования 2-представления в $\mathbb{Z}$ -представление.

Необходимо найти эрмитову нормальную форму блочной матрицы $\begin{pmatrix} A \\ B \end{pmatrix}$, где $A = \text{diag}(p, \dots, p)$, а B является матричным представлением элемента α .

В 1979 г. было доказано, что эрмитову нормальную форму матрицы можно найти за строго полиномиальное время [20]. Это означает, что алгоритму необходимо полиномиальное (относительно размеров матрицы) количество арифметических операций над числами, не превосходящими полинома от бинарного представления элементов матрицы. Таким образом, учитывая, что n зависит только от $\mathcal{O}_K$, эрмитову нормальную форму можно вычислить за $O(P(\log p))$ бинарных операций, где $P(T)$ – некоторый полином. Утверждение доказано.

Замечание 3. Схемы разделения секрета являются составной частью многих криптографических протоколов. В [21–23] представлены новые эффективные схемы верификации модулярного разделения секрета на основе свойств делимости многочленов с целыми коэффициентами или умножения параметров схемы на подходящие случайные величины. Предложенные протоколы могут быть безопасно использованы для многочленов над произвольными конечными полями без дополнительных ограничений на мощность поля.

Замечание 4. Зная разложение (p_i) на произведение простых идеалов, можно найти одинаковые идеалы и разложение $(Nm(N))$ на произведение различных идеалов за $O(P(\log Nm(N)))$ бинарных операций, так как $k \leq \log Nm(N)$ и l_i ограничены константой, зависящей только от $\mathcal{O}_K$. Значит, найти разложение идеала $(Nm(N))$ на произведение различных простых идеалов можно за полиномиальное относительно $\log Nm(N)$ и $\log |N|$ количество бинарных операций, если разложение $Nm(N)$ на множители известно [24–26].

Таким образом, аналог RSA-криптосистемы в некотором смысле не дает никакого выигрыша при использовании в кольцах алгебраических целых числовых полей.

Библиографические ссылки

1. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*. 1978;21(2):120–126. DOI: 10.1145/359340.359342.
2. Li B. Generalizations of RSA public key cryptosystem. *IACR, Cryptology ePrint Archive* [Preprint]. 2005 [cited 2019 August 23]. Available from: <https://arxiv.org/ia.cr/2005/285>.
3. Elkamchouchi H, Elshenawy K, Shaban H. Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers. In: *ICCS 2002. Proceedings of the 8th International conference on communication systems; 2002 November 28; Singapore, Singapore. Volume 1*. [S. l.]: IEEE; 2002. p. 91–95. DOI: 10.1109/ICCS.2002.1182444.
4. Koval A, Verkhovsky B. Analysis of RSA over Gaussian Integers Algorithm. In: *ITNG 2008. Proceedings of the Fifth International conference on information technology: new generations; 2008 April 7–9; Las Vegas, Nevada*. Washington: IEEE Computer Society; 2008. p. 101–105. DOI: 10.1109/ITNG.2008.44.
5. El-Kassar AN, Haraty RA, Awad YA, Debnath NC. Modified RSA in the domains of Gaussian integers and polynomials over finite fields. In: *Proceedings of the ISCA 18th International conference on computer applications in industry and engineering; 2005 November 9–11; Honolulu, Hawaii*. [S. l.]: International Society for Computers and their Applications (ISCA); 2005. p. 298–303.
6. Vaskouski M, Kondratyionok N, Prochorov N. Primes in quadratic unique factorization domains. *Journal of Number Theory*. 2016;168:101–116. DOI: 10.1016/j.jnt.2016.04.022.
7. Petukhova KA, Tronin SN. RSA Cryptosystem for Dedekind rings. *Lobachevskii Journal of Mathematics*. 2016;37:284–287. DOI: 10.1134/S1995080216030197.
8. Brunyate A, Clark PL. Extending the Zolotarev – Frobenius approach to quadratic reciprocity. *The Ramanujan Journal*. 2015; 37(1):25–50. DOI: 10.1007/s11139-014-9635-y.
9. Cohen HA. *Course in computational algebraic number theory*. Berlin: Springer; 1996. 545 p.
10. Cohen H. *Advanced topics in computational number theory*. New York: Springer; 1999. 599 p.
11. Coppersmith D. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *Journal of Cryptology*. 1997; 10:233–260. DOI: 10.1007/s001459900030.
12. Dedekind R. Über den zusammenhang zwischen der theorie der ideale und der theorie der höheren congruenzen. *Abhandlungen der Königlichen Gesellschaft der Wissenschaften in Göttingen*. 1878;23:3–38.
13. Wikstrom D. On the l -Ary GCD-algorithm in rings of integers. In: Caires L, Italiano GF, Monteiro L, Palamidessi C, Yung M, editors. *Automata, Languages and Programming. 32nd International Colloquium, ICALP; 2005 July 11–15; Lisbon, Portugal*. Berlin: Springer; 2005. p. 1189–1201. DOI: 10.1007/11523468_96.
14. Wiener MJ. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information Theory*. 1990;36(3):553–558. DOI: 10.1109/18.54902.
15. Coron JS, May A. Deterministic polynomial-time equivalence of computing the RSA secret key and factoring. *Journal of Cryptology*. 2007;20(1):39–50. DOI: 10.1007/s00145-006-0433-6.
16. Vaskouski M, Kondratyionok N. Shortest division chains in unique factorization domains. *Journal of Symbolic Computation*. 2016;77:175–188. DOI: 10.1016/j.jsc.2016.02.003.
17. Васьковский ММ. Полиномиальная эквивалентность вычисления функции Эйлера RSA-модуля и поиска секретного ключа в квадратичных евклидовых кольцах. В: *Международный конгресс по информатике: информационные системы и технологии. Материалы Международного научного конгресса; 31 октября – 3 ноября 2011 г.; Минск, Беларусь. Часть 2*. Минск: БГУ; 2016. с. 427–430.
18. Бабуль ОВ, Васильев ДВ. О факторизации идеалов в кольцах целых алгебраических чисел. *Известия Национальной академии наук Беларуси. Серия физико-математических наук*. 2011;1:32–36.
19. Pohst ME. *Computational algebraic number theory*. Basel: Birkhäuser; 1993. 88 p. DOI: 10.1007/978-3-0348-8589-8.
20. Kannan R, Bachem A. Polynomial algorithms for computing the smith and hermite normal forms of an integer matrix. *SIAM Journal on Computing*. 1979;8(4):499–507. DOI: 10.1137/0208040.
21. Васьковский ММ, Матвеев ГВ. Верификация модулярного разделения секрета. *Журнал Белорусского государственного университета. Математика. Информатика*. 2017;2:17–22.
22. Матвеев ГВ, Матулис ВВ. Совершенная верификация модулярной схемы. *Журнал Белорусского государственного университета. Математика. Информатика*. 2018;2:4–9.

23. Матвеев ГВ. Разделение секрета в кольцах многочленов от нескольких переменных с использованием китайской теоремы об остатках. *Журнал Белорусского государственного университета. Математика. Информатика*. 2019;3:129–133. DOI: 10.33581/2520-6508-2019-3-129-133.
24. Гекке Э. *Лекции по теории алгебраических чисел*. Ольшанский ГИ, Райков ДА, переводчики. Москва: Государственное издательство технико-теоретической литературы; 1940. 261 с.
25. Глухов ММ, Круглов ИА, Пичкур АБ, Черемушкин АВ. *Введение в теоретико-числовые методы криптографии*. Санкт-Петербург: Лань; 2011. 400 с.
26. Koblitz N. *Course in number theory and cryptography*. New York: Springer-Verlag; 1994. 235 p.

References

1. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*. 1978;21(2):120–126. DOI: 10.1145/359340.359342.
2. Li B. Generalizations of RSA public key cryptosystem. *IACR, Cryptology ePrint Archive* [Preprint]. 2005 [cited 2019 August 23]. Available from: <https://arxiv.org/ia.cr/2005/285>.
3. Elkamchouchi H, Elshenawy K, Shaban H. Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers. In: *ICCS 2002. Proceedings of the 8th International conference on communication systems; 2002 November 28; Singapore, Singapore. Volume 1*. [S. l.]: IEEE; 2002. p. 91–95. DOI: 10.1109/ICCS.2002.1182444.
4. Koval A, Verkhovsky B. Analysis of RSA over Gaussian Integers Algorithm. In: *ITNG 2008. Proceedings of the Fifth International conference on information technology: new generations; 2008 April 7–9; Las Vegas, Nevada*. Washington: IEEE Computer Society; 2008. p. 101–105. DOI: 10.1109/ITNG.2008.44.
5. El-Kassar AN, Haraty RA, Awad YA, Debnath NC. Modified RSA in the domains of Gaussian integers and polynomials over finite fields. In: *Proceedings of the ISCA 18th International conference on computer applications in industry and engineering; 2005 November 9–11; Honolulu, Hawaii*. [S. l.]: International Society for Computers and their Applications (ISCA); 2005. p. 298–303.
6. Vaskouski M, Kondratyuk N, Prochorov N. Primes in quadratic unique factorization domains. *Journal of Number Theory*. 2016;168:101–116. DOI: 10.1016/j.jnt.2016.04.022.
7. Petukhova KA, Tronin SN. RSA Cryptosystem for Dedekind rings. *Lobachevskii Journal of Mathematics*. 2016;37:284–287. DOI: 10.1134/S1995080216030197.
8. Brunyate A, Clark PL. Extending the Zolotarev – Frobenius approach to quadratic reciprocity. *The Ramanujan Journal*. 2015; 37(1):25–50. DOI: 10.1007/s11139-014-9635-y.
9. Cohen HA. *Course in computational algebraic number theory*. Berlin: Springer; 1996. 545 p.
10. Cohen H. *Advanced topics in computational number theory*. New York: Springer; 1999. 599 p.
11. Coppersmith D. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *Journal of Cryptology*. 1997; 10:233–260. DOI: 10.1007/s001459900030.
12. Dedekind R. Über den zusammenhang zwischen der theorie der ideale und der theorie der höheren congruenzen. *Abhandlungen der Königlichen Gesellschaft der Wissenschaften in Göttingen*. 1878;23:3–38.
13. Wikstrom D. On the l -Ary GCD-algorithm in rings of integers. In: Caires L, Italiano GF, Monteiro L, Palamidessi C, Yung M, editors. *Automata, Languages and Programming. 32nd International Colloquium, ICALP; 2005 July 11–15; Lisbon, Portugal*. Berlin: Springer; 2005. p. 1189–1201. DOI: 10.1007/11523468_96.
14. Wiener MJ. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information Theory*. 1990;36(3):553–558. DOI: 10.1109/18.54902.
15. Coron JS, May A. Deterministic polynomial-time equivalence of computing the RSA secret key and factoring. *Journal of Cryptology*. 2007;20(1):39–50. DOI: 10.1007/s00145-006-0433-6.
16. Vaskouski M, Kondratyuk N. Shortest division chains in unique factorization domains. *Journal of Symbolic Computation*. 2016;77:175–188. DOI: 10.1016/j.jsc.2016.02.003.
17. Vaskouski MM. Polynomial equivalence of computing Euler’s function from RSA modulus and searching for private key in euclidean quadratic domains. In: *International congress on computer science: information systems and technologies. Proceedings of the International scientific congress; 2011 October 31 – November 3; Minsk, Belarus. Part 2*. Minsk: Belarusian State University; 2016. p. 427–430. Russian.
18. Babul OV, Vasilyev DV. [Ideals factorization in the number]. *Proceedings of the National Academy of Sciences of Belarus. Physics and Mathematics Series*. 2011;1:32–36. Russian.
19. Pohst ME. *Computational algebraic number theory*. Basel: Birkhäuser; 1993. 88 p. DOI: 10.1007/978-3-0348-8589-8.
20. Kannan R, Bachem A. Polynomial algorithms for computing the smith and hermite normal forms of an integer matrix. *SIAM Journal on Computing*. 1979;8(4):499–507. DOI: 10.1137/0208040.
21. Vaskouski MM, Matveev GV. Verification of modular secret sharing. *Journal of the Belarusian State University. Mathematics and Informatics*. 2017;2:17–22. Russian.
22. Matveev GV, Matulis VV. Perfect verification of modular scheme. *Journal of the Belarusian State University. Mathematics and Informatics*. 2018;2:4–9. Russian.
23. Matveev GV. Chinese remainder theorem secret sharing in multivariate polynomials. *Journal of the Belarusian State University. Mathematics and Informatics*. 2019;3:129–133. Russian. DOI: 10.33581/2520-6508-2019-3-129-133.
24. Hecke E. *Vorlesung über die theorie der algebraischen zahlen*. Leipzig: Akademische Verlagsgesellschaft; 1923. 264 p.
Russian edition: Hecke E. *Leksii po teorii algebraicheskikh chisel*. Ol’shanskii GI, Raikov DA, translators. Moscow: Gosudarstvennoe izdatel’stvo tekhniko-teoreticheskoi literatury; 1940. 261 p.
25. Glukhov MM, Kруглов ИА, Пичкур АБ, Черемушкин АВ. *Vvedenie v teoretiko-chislovye metody kriptografii* [Introduction to number theoretical methods in cryptography]. Saint Petersburg: Lan’; 2011. 400 p. Russian.
26. Koblitz N. *Course in number theory and cryptography*. New York: Springer-Verlag; 1994. 235 p.

УДК 515.12

О НЕПРЕРЫВНОСТИ ФУНКТОРОВ ВИДА $C(X, Y)$

Г. О. КУКРАК¹⁾, В. Л. ТИМОХОВИЧ¹⁾

¹⁾Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь

Рассматривается категория $\mathcal{P}$, объекты которой – пары топологических пространств (X, Y) . Каждой такой паре ставится в соответствие пространство непрерывных отображений $C_\tau(X, Y)$ с топологией τ . Наложением некоторых ограничений на объекты и морфизмы категории $\mathcal{P}$ выделяется подкатегория $\mathcal{K} \subset \mathcal{P}$, для которой указанное отображение является функтором из $\mathcal{K}$ в категорию Тор топологических пространств и непрерывных отображений. Исследуется вопрос о том, при каких дополнительных условиях на $\mathcal{K}$ указанный функтор непрерывен. При этом решается задача нахождения предела обратного спектра в категории $\mathcal{P}$. Показано, что она сводится к отысканию пределов возникающих естественным образом прямого и обратного спектров в категории Тор. В качестве τ рассмотрены топология поточечной сходимости, компактно-открытая топология и топология графика.

Ключевые слова: пространство отображений; функтор $C(X, Y)$; непрерывный функтор; обратный спектр; прямой спектр.

Образец цитирования:

Кукрак ГО, Тимохович ВЛ. О непрерывности функторов вида $C(X, Y)$. Журнал Белорусского государственного университета. Математика. Информатика. 2020;1:22–29. <https://doi.org/10.33581/2520-6508-2020-1-22-29>

For citation:

Kukrak HO, Timokhovich VL. On the continuity of functors of the type $C(X, Y)$. Journal of the Belarusian State University. Mathematics and Informatics. 2020;1:22–29. Russian. <https://doi.org/10.33581/2520-6508-2020-1-22-29>

Авторы:

Глеб Олегович Кукрак – кандидат физико-математических наук; доцент кафедры геометрии, топологии и методики преподавания математики механико-математического факультета.

Владимир Леонидович Тимохович – кандидат физико-математических наук, доцент; доцент кафедры геометрии, топологии и методики преподавания математики механико-математического факультета.

Authors:

Hleb O. Kukrak, PhD (physics and mathematics); associate professor at the department of geometry, topology and methods of teaching mathematics, faculty of mechanics and mathematics. kukrak@bsu.by

Vladimir L. Timokhovich, PhD (physics and mathematics), doцент; associate professor at the department of geometry, topology and methods of teaching mathematics, faculty of mechanics and mathematics. timvlaleo@gmail.com

ON THE CONTINUITY OF FUNCTORS OF THE TYPE $C(X, Y)$

H. O. KUKRAK^a, V. L. TIMOKHOVICH^a

^aBelarusian State University, 4 Niezaliežnasci Avenue, Minsk 220030, Belarus

Corresponding author: H. O. Kukrak (timvlaleo@gmail.com)

We consider the category $\mathcal{P}$, the objects of which are pairs of topological spaces (X, Y) . Each such pair (X, Y) is assigned the space of continuous maps $C_\tau(X, Y)$ with some topology τ . By imposing some restrictions on objects and morphisms of category $\mathcal{P}$, we define a subcategory $\mathcal{K} \subset \mathcal{P}$, for which the above map is a functor from $\mathcal{K}$ to the category $\mathbf{Top}$ of topological spaces and continuous maps. The following question is investigated. What are the additional conditions on $\mathcal{K}$, under which the above functor is continuous? Along the way the problem of finding the limit of the inverse spectrum in the category $\mathcal{P}$ is solved. We show, that it reduces to finding the limits of the corresponding direct spectrum and inverse spectrum in the category $\mathbf{Top}$. Point convergence topology, compact-open topology and graph topology are considered as the topology τ .

Keywords: function space; functor $C(X, Y)$; continuous functor; inverse spectrum; direct spectrum.

Введение

Рассмотрим категорию $\mathcal{P}$, объектами которой являются произвольные упорядоченные пары (X, Y) топологических пространств, а морфизмом пары (X, Y) в пару (E, Z) – любая упорядоченная пара (φ, ψ) непрерывных отображений $E \xrightarrow{\varphi} X, Y \xrightarrow{\psi} Z$ (композиция $(\varphi', \psi') \circ (\varphi, \psi) = (\varphi \circ \varphi', \psi' \circ \psi)$). Переходя от пар $(X, Y), (E, Z)$ и морфизма $(X, Y) \xrightarrow{(\varphi, \psi)} (E, Z)$ к множествам непрерывных отображений $C(X, Y), C(E, Z)$ (кратко: $C(X)$ при $Y = \mathbb{R}$) и соответствующему отображению $C(X, Y) \xrightarrow{c(\varphi, \psi)} C(E, Z): f \rightarrow \bar{f} = \psi \circ f \circ \varphi$, получаем функтор C из категории $\mathcal{P}$ в категорию $\mathbf{Set}$ всех множеств и отображений. При задании на множествах вида $C(X, Y)$ некоторой топологии τ естественно возникает задача отыскания достаточно обширной подкатегории $\mathcal{K}$ в $\mathcal{P}$, в рамках которой любое отображение вида $C(X, Y) \xrightarrow{c(\varphi, \psi)} C(E, Z)$ непрерывно, и тогда C – функтор из $\mathcal{K}$ в категорию $\mathbf{Top}$ топологических пространств и непрерывных отображений.

Исследования в указанном направлении начаты в работе [1], которая, в свою очередь, предваряется статьями [2–5]. В настоящей статье они продолжены. В качестве τ рассмотрены топология поточечной сходимости τ_p , компактно-открытая топология τ_k и топология графика τ_Γ , а соответствующие функторы в категорию $\mathbf{Top}$ исследованы на непрерывность.

Понятия и обозначения

Пусть X – топологическое пространство (далее – просто пространство), $A \subset X, x \in X$. Обозначим: τ_X – топология пространства X , $\tau_X(A) = \{U \in \tau_X \mid A \subset U\}$, $\tau_X(x) = \tau_X(\{x\})$; id_X – тождественное отображение X на себя.

Пространство X называют:

- k -пространством [6, с. 236], если из того, что A не замкнуто, следует существование компактного множества $B \subset X$, для которого $A \cap B$ не замкнуто в B ;
- изокомпактным [7], если компактно любое счетно-компактное замкнутое множество $B \subset X$ (таково, например, любое слабо паракомпактное пространство [6, с. 477]).

Отображение $f \in C(X, Y)$ называют:

- совершенным [6, с. 277], если оно замкнуто (т. е. $f(F)$ замкнуто в Y для любого замкнутого $F \subset X$) и $f^{-1}(y)$ компактно для любой точки $y \in Y$;
- k -накрывающим [6, с. 506], если для каждого компактного $B \subset Y$ найдется компактное $F \subset X$, для которого $f(F) = B$. Всякое совершенное сюръективное отображение является k -накрывающим [6, с. 278].

Отметим, что, в отличие от [6], в определениях k -пространства и совершенного и k -накрывающего отображений никакие условия отделимости нами не предполагаются.

На множестве $C(X, Y)$ топология поточечной сходимости τ_p [6, с. 172], компактно-открытая топология τ_k [6, с. 243] и топология графика τ_Γ [8] определены предбазами, состоящими из всех множеств вида $\langle x, V \rangle = \{f \in C(X, Y) \mid f(x) \in V\}$ (для τ_p), $\langle F, V \rangle = \{f \in C(X, Y) \mid f(F) \subset V\}$ (для τ_k) и $O(U) = \{f \in C(X, Y) \mid \Gamma_f \in U\}$ (для τ_Γ), где $x \in X$, $F \subset X$ и F компактно, $V \in \tau_Y$, $\Gamma_f = \{(x, f(x)) \in X \times Y \mid x \in X\}$ – график отображения f и U – открытое множество в $X \times Y$. Соответствующие пространства обозначаем кратко через $C_p(X, Y)$, $C_k(X, Y)$ и $C_\Gamma(X, Y)$.

Пусть $\mathcal{A}$ – некоторая категория, множество Σ направлено (т. е. частично упорядочено и для любых $\alpha, \beta \in \Sigma$ можно выбрать $\gamma \in \Sigma$ так, что $\gamma \geq \alpha$ и $\gamma \geq \beta$) и для каждого $\alpha \in \Sigma$ и $\beta \geq \alpha$ определены объект X_α и морфизм φ_α^β из $\mathcal{A}$. Семейство S указанных объектов и связующих морфизмов обозначают кратко $S = \{X_\alpha, \varphi_\alpha^\beta, \Sigma\}$ и называют *обратным спектром* или *проективной системой* [9, с. 89; 10, с. 59] (*прямым спектром* или *индуктивной системой* [10, с. 59]), если φ_α^α есть тождественный морфизм 1_{X_α} , $\varphi_\alpha^\beta : X_\beta \rightarrow X_\alpha$ ($\varphi_\alpha^\beta : X_\alpha \rightarrow X_\beta$ соответственно) и $\varphi_\alpha^\gamma = \varphi_\alpha^\beta \circ \varphi_\beta^\gamma$ ($\varphi_\alpha^\gamma = \varphi_\beta^\gamma \circ \varphi_\alpha^\beta$) при $\alpha \leq \beta \leq \gamma$.

Под *пределом* в категории $\mathcal{A}$ обратного (прямого) спектра S понимают объект X в совокупности с морфизмами $\pi_\alpha : X \rightarrow X_\alpha$ ($\pi_\alpha : X_\alpha \rightarrow X$), удовлетворяющими условиям:

(а) $\pi_\alpha = \varphi_\alpha^\beta \circ \pi_\beta$ ($\pi_\alpha = \pi_\beta \circ \varphi_\alpha^\beta$) при $\alpha \leq \beta$;

(б) если объект X' из $\mathcal{A}$ и морфизмы $\pi'_\alpha : X' \rightarrow X_\alpha$ ($\pi'_\alpha : X_\alpha \rightarrow X'$) таковы, что $\pi'_\alpha = \varphi_\alpha^\beta \circ \pi'_\beta$ ($\pi'_\alpha = \pi'_\beta \circ \varphi_\alpha^\beta$) при $\alpha \leq \beta$, то существует единственный морфизм $h : X' \rightarrow X$ ($h : X \rightarrow X'$), для которого $\pi'_\alpha = \pi_\alpha \circ h$ ($\pi'_\alpha = h \circ \pi_\alpha$) при любом $\alpha \in \Sigma$. Если спектр S обратный, то его предел обозначают $\varprojlim S$ или $\varprojlim X_\alpha$, если прямой, то $\varinjlim S$ или $\varinjlim X_\alpha$, а морфизмы π_α называют (в обоих случаях) *каноническими проекциями*.

В категории Тор пределы спектров существуют и определены следующим образом. Если спектр S обратный, то его предел – подпространство $L \subset \prod_{\alpha \in \Sigma} X_\alpha$, $L = \{(x_\alpha \mid \alpha \in \Sigma) \mid x_\alpha = \varphi_\alpha^\beta(x_\beta), \alpha \leq \beta\}$, а морфизмы π_α – естественные проекции $L \xrightarrow{\pi_\alpha} X_\alpha$. Элементы L называют *нитеями спектра* S . Базу в L образуют множества вида $\pi_\alpha^{-1}(V)$, где $V \in \tau_{X_\alpha}$ [9, с. 90]. Предел прямого спектра S – фактор-пространство K дискретной суммы $\coprod_{\alpha \in \Sigma} X_\alpha$ по следующему отношению эквивалентности: $x \sim y$ ($x \in X_\alpha, y \in X_\beta$), если $\varphi_\alpha^\gamma(x) = \varphi_\beta^\gamma(y)$ при некотором $\gamma \in \Sigma$, а канонические проекции $X_\alpha \rightarrow K$ (их обозначаем через ι_α) определены как сужения $\iota_\alpha = \pi|_{X_\alpha}$, где $\pi : \coprod_{\alpha \in \Sigma} X_\alpha \rightarrow K$ – естественная проекция.

Пусть $\mathcal{A}$ и $\mathcal{B}$ – категории, $\mathcal{F} : \mathcal{A} \rightarrow \mathcal{B}$ – ковариантный функтор, $S = \{X_\alpha, \varphi_\alpha^\beta, \Sigma\}$ – обратный спектр в $\mathcal{A}$, имеющий в $\mathcal{A}$ предел $L = \varprojlim X_\alpha$ с каноническими проекциями $L \xrightarrow{\pi_\alpha} X_\alpha$. В категории $\mathcal{B}$ определены соответствующие обратный спектр $\mathcal{F}(S) = \{\mathcal{F}(X_\alpha), \mathcal{F}(\varphi_\alpha^\beta), \Sigma\}$, объект $\mathcal{F}(L)$ и морфизмы $\mathcal{F}(\pi_\alpha) : \mathcal{F}(L) \rightarrow \mathcal{F}(X_\alpha)$, причем $\mathcal{F}(\pi_\alpha) = \mathcal{F}(\varphi_\alpha^\beta) \circ \mathcal{F}(\pi_\beta)$ при $\alpha \leq \beta$. Функтор $\mathcal{F}$ называют *непрерывным* или *перестановочным с обратным пределом* [9, с. 187; 10, с. 64], если для любого такого S объект $\mathcal{F}(L)$ в совокупности с морфизмами $\mathcal{F}(\pi_\alpha) : \mathcal{F}(L) \rightarrow \mathcal{F}(X_\alpha)$ является пределом обратного спектра $\mathcal{F}(S)$ в категории $\mathcal{B}$.

Функторы C_p , C_k и C_Γ

Задавая на множествах вида $C(X, Y)$ некоторую топологию τ , мы ставим в соответствие каждому объекту (X, Y) категории $\mathcal{P}$ топологическое пространство $C_\tau(X, Y)$. Если при этом для любого морфизма $(X, Y) \xrightarrow{(\varphi, \psi)} (E, Z)$ из некоторой подкатегории $\mathcal{K} \subset \mathcal{P}$ соответствующее отображение $C_\tau(X, Y) \xrightarrow{c(\varphi, \psi)} C_\tau(E, Z) : f \mapsto \bar{f} = \psi \circ f \circ \varphi$ непрерывно, то получаем ковариантный функтор C_τ из $\mathcal{K}$ в категорию Тор. Далее в качестве τ рассмотрим топологии τ_p , τ_k и τ_Γ , а соответствующие функторы обозначим кратко через C_p , C_k и C_Γ . Нам понадобятся следующие из полученных ранее результатов.

Теорема 1 [1]. *Отображения $C_p(X, Y) \xrightarrow{c(\varphi, \psi)} C_p(E, Z)$ и $C_\kappa(X, Y) \xrightarrow{c(\varphi, \psi)} C_\kappa(E, Z)$ непрерывны при любых $X, Y, E, Z, \varphi \in C(E, X)$ и $\psi \in C(Y, Z)$.*

Следствие 1. C_p и C_κ – функторы из категории $\mathcal{P}$ в категорию Tor .

Теорема 2 [1]. *Если отображение $\varphi \in C(E, X)$ совершенно, то $C_\Gamma(X, Y) \xrightarrow{c(\varphi, \psi)} C_\Gamma(E, Z)$ непрерывно для любых Y, Z и $\psi \in C(Y, Z)$.*

Следствие 2. Пусть $\mathcal{K}$ – подкатегория в $\mathcal{P}$, в которой для каждого морфизма (φ, ψ) отображение φ совершенно. Тогда C_Γ – функтор из $\mathcal{K}$ в категорию Tor .

При непрерывности отображений вида $C_\Gamma(X, Y) \xrightarrow{c(\varphi, \psi)} C_\Gamma(E, Z)$ вопрос (обратный) о совершенности $\varphi \in C(E, X)$ решается следующим образом.

Теорема 3 [1]. *Отображение $\varphi \in C(E, X)$ совершенно, если отображение $C_\Gamma(X, \mathbb{R}) \xrightarrow{c(\varphi, \text{id}_\mathbb{R})} C_\Gamma(E, \mathbb{R})$ непрерывно, E изомактно, а X – вполне регулярное k -пространство.*

Следствие 3. Пусть $\mathcal{K}$ – подкатегория в $\mathcal{P}$, в которой для любого объекта (X, Y) пространство X – вполне регулярное и изомактно k -пространство, и вместе с каждым морфизмом $(X, Y) \xrightarrow{(\varphi, \psi)} (E, Z)$ содержится также морфизм $(X, \mathbb{R}) \xrightarrow{(\varphi, \text{id}_\mathbb{R})} (E, \mathbb{R})$. Если при этом C_Γ является функтором из $\mathcal{K}$ в категорию Tor , то для любого морфизма (φ, ψ) из $\mathcal{K}$ отображение φ совершенно.

Непрерывность функторов C_p, C_κ и C_Γ

В категории $\mathcal{P}$ рассмотрим обратный спектр $S = \{(X_\alpha, Y_\alpha), (\varphi_\alpha^\beta, \psi_\alpha^\beta), \Sigma\}$ и соответствующие спектры в категории Tor : прямой спектр $S_X = \{X_\alpha, \varphi_\alpha^\beta, \Sigma\}$ и обратный спектр $S_Y = \{Y_\alpha, \psi_\alpha^\beta, \Sigma\}$. Пусть $K = \varprojlim X_\alpha$ и $L = \varprojlim Y_\alpha$ – их пределы, $\iota_\alpha : X_\alpha \rightarrow K$ и $\pi_\alpha : L \rightarrow Y_\alpha$ – соответствующие канонические проекции. Возвращаясь в $\mathcal{P}$, получим пару (K, L) и дополнительно к морфизмам $(X_\beta, Y_\beta) \xrightarrow{(\varphi_\alpha^\beta, \psi_\alpha^\beta)} (X_\alpha, Y_\alpha)$ также морфизмы $(K, L) \xrightarrow{(\iota_\alpha, \pi_\alpha)} (X_\alpha, Y_\alpha)$, причем $(\iota_\alpha, \pi_\alpha) = (\varphi_\alpha^\beta, \psi_\alpha^\beta) \circ (\iota_\beta, \pi_\beta)$ при $\alpha \leq \beta$. Пусть далее пара (K', L') и морфизмы $(K', L') \xrightarrow{(\iota'_\alpha, \pi'_\alpha)} (X_\alpha, Y_\alpha)$ таковы, что $(\iota'_\alpha, \pi'_\alpha) = (\varphi_\alpha^\beta, \psi_\alpha^\beta) \circ (\iota'_\beta, \pi'_\beta)$ при $\alpha \leq \beta$.

Очевидно, что для отображений $\iota'_\alpha : X_\alpha \rightarrow K'$ и $\pi'_\alpha : L' \rightarrow Y_\alpha$ выполняются соотношения $\iota'_\alpha = \iota'_\beta \circ \varphi_\alpha^\beta$ и $\pi'_\alpha = \pi'_\beta \circ \psi_\alpha^\beta$ при $\alpha \leq \beta$ и, следовательно, определены однозначно непрерывные отображения $K \xrightarrow{u} K'$ и $L' \xrightarrow{v} L$ такие, что $\iota'_\alpha = u \circ \iota_\alpha$ и $\pi'_\alpha = \pi_\alpha \circ v$ для любого $\alpha \in \Sigma$. Но тогда морфизм $(K', L') \xrightarrow{(u, v)} (K, L)$ единственный, для которого $(\iota'_\alpha, \pi'_\alpha) = (\iota_\alpha, \pi_\alpha) \circ (u, v)$ при всех $\alpha \in \Sigma$. Итак, условия (a) и (b) категорного определения предела обратного спектра проверены и таким образом доказана следующая теорема.

Теорема 4. В категории $\mathcal{P}$ пределом обратного спектра $S = \{(X_\alpha, Y_\alpha), (\varphi_\alpha^\beta, \psi_\alpha^\beta), \Sigma\}$ является пара (K, L) , где $K = \varprojlim X_\alpha$, $L = \varprojlim Y_\alpha$, а каноническими проекциями – морфизмы $(K, L) \xrightarrow{(\iota_\alpha, \pi_\alpha)} (X_\alpha, Y_\alpha)$, где ι_α и π_α – канонические проекции пределов (в категории Tor) K и L соответственно.

Отметим, что категория $\mathcal{P}$ является произведением категории Tor и дуальной категории Tor^* (полученной «поворотом стрелок»), $\mathcal{P} = \text{Tor}^* \times \text{Tor}$, и теореме 4 можно доказать как простое утверждение в рамках общей теории категорий.

Рассмотрим тот же обратный спектр $S = \{(X_\alpha, Y_\alpha), (\varphi_\alpha^\beta, \psi_\alpha^\beta), \Sigma\}$. Предположим, что некоторая подкатегория $\mathcal{K} \subset \mathcal{P}$ содержит все объекты спектра S , пару $(K, L) = \varprojlim (X_\alpha, Y_\alpha)$ и все морфизмы $(\varphi_\alpha^\beta, \psi_\alpha^\beta)$ и $(\iota_\alpha, \pi_\alpha)$, и при задании на множествах вида $C(X, Y)$ топологии τ возникает функтор C_τ из $\mathcal{K}$ в категорию Tor . Теперь рассмотрим соответствующие обратный спектр $C_\tau(S) = \{C_\tau(X_\alpha, Y_\alpha), c(\varphi_\alpha^\beta, \psi_\alpha^\beta), \Sigma\}$ (в категории Tor), его предел $\Lambda = \varprojlim C_\tau(X_\alpha, Y_\alpha)$ с каноническими проекциями $\Pi_\alpha : \Lambda \rightarrow C_\tau(X_\alpha, Y_\alpha)$, пространство $C_\tau(K, L)$ и непрерывные отображения $C_\tau(K, L) \xrightarrow{c(\iota_\alpha, \pi_\alpha)} C_\tau(X_\alpha, Y_\alpha)$. Поскольку $c(\iota_\alpha, \pi_\alpha) = c(\varphi_\alpha^\beta, \psi_\alpha^\beta) \circ c(\iota_\beta, \pi_\beta)$ при $\alpha \leq \beta$, то определено, причем единственным образом, непрерывное отображение $h : C_\tau(K, L) \rightarrow \Lambda$ такое, что $c(\iota_\alpha, \pi_\alpha) = \Pi_\alpha \circ h$ для всех $\alpha \in \Sigma$.

Лемма 1. Пусть $f \in C_\tau(K, L)$ и $h(f) = (f_\alpha | \alpha \in \Sigma) (f_\alpha = \Pi_\alpha(h(f)) \in C_\tau(X_\alpha, Y_\alpha))$. Тогда $f_\alpha = \pi_\alpha \circ f \circ \iota_\alpha$, $\alpha \in \Sigma$.

Доказательство следует непосредственно из равенства $c(\iota_\alpha, \pi_\alpha) = \Pi_\alpha \circ h$.

Лемма 2. Отображение $h : C_\tau(K, L) \rightarrow \Lambda$ – непрерывная биекция.

Доказательство. Непрерывность h уже отмечена. Докажем биективность. Для этого сперва покажем инъективность. Пусть $f, g \in C(K, L)$, $h(f) = (f_\alpha | \alpha \in \Sigma)$, $h(g) = (g_\alpha | \alpha \in \Sigma)$ и $f \neq g$. Тогда для некоторого класса эквивалентности $[x_\beta] \in K$ ($x_\beta \in X_\beta$) нити $f([x_\beta]) = (y_\alpha | \alpha \in \Sigma)$ и $g([x_\beta]) = (z_\alpha | \alpha \in \Sigma)$ различны, т. е. $y_\gamma \neq z_\gamma$ для некоторого $\gamma \in \Sigma$. Выберем $\delta \in \Sigma$ такое, что $\delta \geq \beta$ и $\delta \geq \gamma$, и обозначим $x_\delta = \phi_\beta^\delta(x_\beta)$ ($x_\delta \in X_\delta$). Используя лемму 1 и соотношение $[x_\delta] = [x_\beta]$, получим $f_\delta(x_\delta) = (\pi_\delta \circ f \circ \iota_\delta)(x_\delta) = y_\delta$ и $g_\delta(x_\delta) = (\pi_\delta \circ g \circ \iota_\delta)(x_\delta) = z_\delta$. Но $y_\delta \neq z_\delta$, поскольку $\psi_\gamma^\delta(y_\delta) = y_\gamma \neq z_\gamma = \psi_\gamma^\delta(z_\delta)$. Итак, $f_\delta \neq g_\delta$, т. е. $h(f) \neq h(g)$. Инъективность доказана.

Пусть теперь $(f_\alpha | \alpha \in \Sigma) \in \Lambda$. Покажем существование $f \in C_\tau(K, L)$ такого, что $h(f) = (f_\alpha | \alpha \in \Sigma)$, т. е. $f_\alpha = \pi_\alpha \circ f \circ \iota_\alpha$, $\alpha \in \Sigma$ (см. лемму 1). Для произвольных $\gamma, \alpha \in \Sigma$ выберем $\delta \in \Sigma$, $\delta \geq \gamma$, $\delta \geq \alpha$, и положим $f_{\gamma\alpha} = \psi_\alpha^\delta \circ f_\delta \circ \phi_\gamma^\delta$. Проверим корректность определения. Пусть $\kappa \in \Sigma$, $\kappa \geq \gamma$ и $\kappa \geq \alpha$. Покажем, что $\psi_\alpha^\kappa \circ f_\kappa \circ \phi_\gamma^\kappa = \psi_\alpha^\delta \circ f_\delta \circ \phi_\gamma^\delta$. Подберем $\nu \in \Sigma$ так, чтобы выполнялись соотношения $\nu \geq \delta$ и $\nu \geq \kappa$. Тогда $\psi_\alpha^\kappa \circ f_\kappa \circ \phi_\gamma^\kappa = \psi_\alpha^\kappa \circ \psi_\kappa^\nu \circ f_\nu \circ \phi_\kappa^\nu \circ \phi_\gamma^\kappa = \psi_\alpha^\kappa \circ f_\nu \circ \phi_\gamma^\nu$. С другой стороны, $\psi_\alpha^\delta \circ f_\delta \circ \phi_\gamma^\delta = \psi_\alpha^\delta \circ \psi_\delta^\nu \circ f_\nu \circ \phi_\delta^\nu \circ \phi_\gamma^\delta = \psi_\alpha^\delta \circ f_\nu \circ \phi_\gamma^\nu$. Корректность доказана.

Отметим, что $f_{\gamma\gamma} = f_\gamma$. Для проверки соотношения $f_{\gamma\alpha} = \psi_\alpha^\beta \circ f_{\delta\beta} \circ \phi_\gamma^\delta$ при $\gamma \leq \delta$ и $\alpha \leq \beta$ выберем $\nu \in \Sigma$, $\nu \geq \beta$, $\nu \geq \gamma$, и получим $\psi_\alpha^\beta \circ f_{\delta\beta} \circ \phi_\gamma^\delta = \psi_\alpha^\beta \circ \psi_\beta^\nu \circ f_\nu \circ \phi_\delta^\nu \circ \phi_\gamma^\delta = \psi_\alpha^\beta \circ f_\nu \circ \phi_\gamma^\nu = f_{\gamma\alpha}$. Таким образом, определены непрерывные отображения $f_{\gamma L} : X_\gamma \rightarrow L$, $f_{\gamma L}(x_\gamma) = (f_{\gamma\alpha}(x_\gamma) | \alpha \in \Sigma)$ и $f_{\gamma L} = f_{\nu L} \circ \phi_\gamma^\nu$ при $\gamma \leq \nu$. Но тогда по определению существует единственное непрерывное отображение $f : K \rightarrow L$, для которого $f_{\gamma L} = f \circ \iota_\gamma$ при любом $\gamma \in \Sigma$. А поскольку $\pi_\alpha \circ f \circ \iota_\alpha = \pi_\alpha \circ f_{\alpha L} = f_{\alpha\alpha} = f_\alpha$, то в силу леммы 1 отображение f – искомое. Итак, h сюръективно. Лемма 2 доказана.

Следствие 4. Функтор C_τ непрерывен на категории $\mathcal{K}$ тогда и только тогда, когда обратное отображение $h^{-1} : \Lambda \rightarrow C_\tau(K, L)$ непрерывно при любом выборе в $\mathcal{K}$ обратного спектра S , для которого в $\mathcal{K}$ существует предел $(K, L) = \varinjlim S$.

Теорема 5. Функтор C_p из категории $\mathcal{P}$ в категорию Тор непрерывен.

Доказательство. Учитывая следствие 4, рассмотрим произвольные $f \in C_p(K, L)$ и окрестность f вида $\langle [x_\gamma], \pi_\beta^{-1}(V_\beta) \rangle$, где $[x_\gamma] \in K$ ($x_\gamma \in X_\gamma$), V_β открыто в Y_β . Пусть $f([x_\gamma]) = (y_\alpha | \alpha \in \Sigma) \in L$. Ясно, что $y_\beta \in V_\beta$. Выберем $\delta \in \Sigma$, $\delta \geq \gamma$, $\delta \geq \beta$, и обозначим $x_\delta = \phi_\gamma^\delta(x_\gamma)$ ($x_\delta \in X_\delta$). Затем в Y_δ выберем окрестность V_δ точки y_δ так, чтобы выполнялось включение $\psi_\beta^\delta(V_\delta) \subset V_\beta$. Перейдем к нити (в Λ) $h(f) = (f_\alpha | \alpha \in \Sigma)$. Заметим (см. лемму 1), что $f_\delta(x_\delta) = \pi_\delta(f([x_\delta])) = \pi_\delta(f([x_\gamma])) = y_\delta \in V_\delta$ и, следовательно, $\Pi_\delta^{-1}(\langle x_\delta, V_\delta \rangle)$ – окрестность в Λ нити $h(f)$. Пусть $g \in C_p(K, L)$, $h(g) = (g_\alpha | \alpha \in \Sigma) \in \Pi_\delta^{-1}(\langle x_\delta, V_\delta \rangle)$. Тогда $g_\delta(x_\delta) = \pi_\delta(g([x_\delta])) = \pi_\delta(g([x_\gamma])) \in V_\delta$, откуда $g \in \langle [x_\gamma], \pi_\delta^{-1}(V_\delta) \rangle$. Но $\pi_\delta^{-1}(V_\delta) \subset \pi_\beta^{-1}(V_\beta)$, значит, $\langle [x_\gamma], \pi_\delta^{-1}(V_\delta) \rangle \subset \langle [x_\gamma], \pi_\beta^{-1}(V_\beta) \rangle$, что влечет $g \in \langle [x_\gamma], \pi_\beta^{-1}(V_\beta) \rangle$. Итак, h^{-1} непрерывно. Теорема 5 доказана.

Перейдем к топологии τ_κ .

Лемма 3 [1] (см. также [9, с. 100]). Если $\{Y_\alpha, \psi_\alpha^\beta, \Sigma\}$ – обратный спектр в категории Тор , $L = \varinjlim Y_\alpha$,

$F \subset U \subset L$, U открыто в L , а F компактно, то $F \subset \pi_\beta^{-1}(W) \subset U$ для некоторых $\beta \in \Sigma$ и открытого $W \subset Y_\beta$.

Теорема 6. Пусть $\mathcal{K}$ – подкатегория в $\mathcal{P}$ и для любого морфизма (ϕ, ψ) из $\mathcal{K}$ отображение ϕ k -накрывающее. Тогда функтор C_κ непрерывен на $\mathcal{K}$.

Доказательство. Фиксируем произвольные $f \in C_\kappa(K, L)$ и окрестность f вида $\langle F, G \rangle$, где $F \subset K$ и F компактно, G открыто в L . Учитывая лемму 3 и компактность $f(F)$, считаем, что $G = \pi_\beta^{-1}(V)$, где V открыто в Y_β . Выберем компактное $B \subset X_\beta$ такое, что $\iota_\beta(B) = F$, и рассмотрим нить $h(f) = (f_\alpha | \alpha \in \Sigma) \in \Lambda$, где $\Lambda = \varprojlim C_\kappa(X_\alpha, Y_\alpha)$. Поскольку $f_\beta(B) = (\pi_\beta \circ f \circ \iota_\beta)(B) \subset V$, то $h(f) \in \Pi_\beta^{-1}(\langle B, V \rangle)$. Пусть теперь $g \in C_\kappa(K, L)$, $h(g) = (g_\alpha | \alpha \in \Sigma) \in \Pi_\beta^{-1}(\langle B, V \rangle)$. Ясно, что $(\pi_\beta \circ g)(F) = (\pi_\beta \circ g \circ \iota_\beta)(B) = g_\beta(B) \subset V$, откуда $g \in \langle F, \pi_\beta^{-1}(V) \rangle$. Таким образом, непрерывность h^{-1} проверена и теорема 6 доказана.

Мотивацией выбора k -накрывающих отображений может служить следующее утверждение.

Утверждение. Пусть в подкатегории $\mathcal{K} \subset \mathcal{P}$ для любого объекта (X, Y) пространство X вполне регулярно, вместе с любым морфизмом $(\varphi, \psi) : (X, Y) \rightarrow (E, Z)$ присутствует и морфизм $(\varphi, \text{id}_\mathbb{R}) : (X, \mathbb{R}) \rightarrow (E, \mathbb{R})$ и функтор C_κ непрерывен на $\mathcal{K}$. Тогда если в $\mathcal{K}$ определены обратный спектр $\{(X_\alpha, Y_\alpha), (\varphi_\alpha^\beta, \psi_\alpha^\beta), \Sigma\}$ и его предел (K, L) ($K = \varprojlim X_\alpha$, $L = \varprojlim Y_\alpha$), то для некоторого $\beta \in \Sigma$ все отображения $\iota_\alpha : X_\alpha \rightarrow K$ k -накрывающие при $\alpha \geq \beta$.

Доказательство. Будем считать, что $Y_\alpha = \mathbb{R}$ и $\psi_\alpha^\beta = \text{id}_\mathbb{R}$ при $\alpha \leq \beta$ (в рамках $\mathcal{K}$ такой переход возможен). Ясно, что $L = \mathbb{R}$ и $\pi_\alpha = \text{id}_\mathbb{R}$ для любого $\alpha \in \Sigma$. Пусть $F \subset K$ и F компактно. Рассмотрим $f \in C_\kappa(K, L)$, $f(K) = \{0\}$, нить $h(f) = (f_\alpha | \alpha \in \Sigma) \in \Lambda$, где $\Lambda = \varprojlim C_\kappa(X_\alpha, Y_\alpha)$, и окрестность $\langle F, \left(-\frac{1}{2}; \frac{1}{2}\right) \rangle$ в $C_\kappa(K, L)$ функции f . По условию существуют $\beta \in \Sigma$ и окрестность G в $C_\kappa(X_\beta, Y_\beta)$ функции f_β такие, что $h^{-1}(\Pi_\beta^{-1}(G)) \subset \langle F, \left(-\frac{1}{2}; \frac{1}{2}\right) \rangle$. Поскольку $f_\beta(X_\beta) = \{0\}$, можно считать, что $G = \langle B, (-\varepsilon; \varepsilon) \rangle$, где $B \subset X_\beta$ и B компактно, $\varepsilon > 0$. Покажем, что $F \subset \iota_\beta(B)$. Допустим, что найдется точка $z \in F \setminus \iota_\beta(B)$. Выберем функцию $g \in C(K)$ такую, чтобы выполнялись равенства $g(x) = 0$ при $x \in \iota_\beta(B)$ и $g(z) = 1$. Очевидно, $h(g) \in \Pi_\beta^{-1}(G)$, но $g \notin \langle F, \left(-\frac{1}{2}; \frac{1}{2}\right) \rangle$. Получено противоречие, значит, $F \subset \iota_\beta(B)$. Обозначим $P = B \cap \iota_\beta^{-1}(F)$. Множество P компактно, и $\iota_\beta(P) = F$. Итак, ι_β — k -накрывающее. Но тогда и ι_α — k -накрывающее при $\alpha \geq \beta$ в силу соотношения $\iota_\beta = \iota_\alpha \circ \varphi_\alpha^\beta$. Утверждение доказано.

В завершение рассмотрим топологию τ_Γ на $C(X, Y)$, отдельные свойства которой, в частности связь с топологиями равномерной сходимости при метризуемом Y , были установлены в [2; 5]. В [1] получено необходимое условие непрерывности функтора C_Γ на некоторой подкатегории $\mathcal{K} \subset \mathcal{P}$.

Теорема 7 [1]. Пусть $\mathcal{K}$ — подкатегория в $\mathcal{P}$, в которой вместе с любым объектом (X, Y) присутствует и любой объект вида $(X, W_0(\theta))$, где θ — бесконечный начальный ординал и $W_0(\theta)$ — множество всех ординалов $\alpha \leq \theta$ с порядковой топологией, и для каждого морфизма $(X, Y) \xrightarrow{(\varphi, \psi)} (E, Z)$ непременно $E = X$ и $\varphi = \text{id}_X$. Если при этом функтор C_Γ непрерывен на $\mathcal{K}$, то для любого объекта (X, Y) из $\mathcal{K}$ пространство X компактно.

Пример. Пусть Σ — семейство некоторых непустых замкнутых в $\mathbb{R}$ множеств $A \subset I = [0; 1]$ такое, что $\cup \Sigma = I$, $|A| \leq \omega$ ($\omega = |\mathbb{N}|$) и $A \cup B \in \Sigma$ для любых $A, B \in \Sigma$, и если $(x_n | n \in \mathbb{N})$ — сходящаяся последовательность точек из I , то $\{x_n | n \in \mathbb{N}\} \subset A$ для некоторого $A \in \Sigma$. Положим $A \leq B$, если $A \subset B$; $X_A = A$ (с евклидовой топологией) и $\varphi_A^B : X_A \rightarrow X_B$ — обычное вложение при $A \leq B$; $Y_A = \mathbb{R}$ и $\psi_A^B = \text{id}_\mathbb{R}$ при $A \leq B$. Ясно, что $K = \varprojlim X_A = I$ (с евклидовой топологией) и $\iota_A : X_A \rightarrow K$ — обычное вложение (о подобных примерах см. [11, с. 188]), $L = \varprojlim Y_A = \mathbb{R}$ и $\pi_A = \text{id}_\mathbb{R}$ для любого $A \in \Sigma$. Рассмотрим $f \in C_\Gamma(K, L)$, $f(K) = \{0\}$, $h(f) = (f_A | A \in \Sigma) \in \Lambda$, где $\Lambda = \varprojlim C_\Gamma(X_A, Y_A)$, и окрестность $O(U)$ в $C_\Gamma(K, L)$ функции f , где $U = I \times \left(-\frac{1}{2}; \frac{1}{2}\right)$. Допустим, что существует окрестность нити $h(f)$ вида $\Pi_B^{-1}(O(G))$ (G открыто

в $X_B \times \mathbb{R}$, для которой $h^{-1}(\Pi_B^{-1}(O(G))) \subset O(U)$. Поскольку $f_B(X_B) = \{0\}$ и $X_B = B$ компактно, можно считать, что $G = X_B \times (-\varepsilon; \varepsilon)$, $\varepsilon > 0$. Выберем функцию $g \in C(I)$ так, чтобы выполнялись равенства $g(B) = \{0\}$ и $g(x) = 1$ для некоторой точки $x \in I \setminus B$. Ясно, что $g_B = g \circ \iota_B \in O(G)$, следовательно, $h(g) \in \Pi_B^{-1}(O(G))$. Но поскольку $g \notin O(U)$, то h^{-1} разрывно.

С учетом следствия 2, теоремы 7 и примера представляются разумными следующие ограничения на подкатегорию $\mathcal{K} \subset \mathcal{P}$ в «области непрерывности» C_Γ .

Теорема 8. Пусть в подкатегории $\mathcal{K} \subset \mathcal{P}$ для любого морфизма $(X, Y) \xrightarrow{(\varphi, \psi)} (E, Z)$ пространства X и E компактны, φ – совершенная сюръекция. Тогда функтор C_Γ непрерывен на $\mathcal{K}$.

Доказательство. Фиксируем произвольные $f \in C_\Gamma(K, L)$ ($K = \varinjlim X_\alpha$, $L = \varinjlim Y_\alpha$) и окрестность $O(G)$ отображения f (G открыто в $K \times L$). Для каждой точки $(k, f(k)) \in \Gamma_f$ подберем окрестности U_k точки k и $V(k)$ точки $f(k)$, где $V(k) = \pi_{\alpha(k)}^{-1}(W(k))$, $W(k)$ открыто в $Y_{\alpha(k)}$, так, чтобы выполнялись включения $f(U_k) \subset V(k)$ и $U_k \times V(k) \subset G$. В силу компактности K существует конечное семейство окрестностей $U_{k_1}, \dots, U_{k_n}$ такое, что $\bigcup_{i=1}^n U_{k_i} = K$. Выберем $\gamma \in \Sigma$, чтобы выполнялись соотношения $\gamma \geq \alpha(k_1), \dots, \gamma \geq \alpha(k_n)$. Отметим, что $\pi_\alpha^{-1}(A) = \pi_\beta^{-1}((\psi_\alpha^\beta)^{-1}(A))$, где $A \subset Y_\alpha$ и $\alpha \leq \beta$ произвольные. Обозначив $H_i = (\psi_{\alpha(k_i)}^\gamma)^{-1}(W(k_i))$ (H_i открыто в Y_γ), получим $V(k_i) = \pi_\gamma^{-1}(H_i)$ и $\Gamma_f \subset \bigcup_{i=1}^n (U_{k_i} \times V(k_i)) = \bigcup_{i=1}^n (U_{k_i} \times \pi_\gamma^{-1}(H_i)) \subset G$. Далее положим $Q_i = \iota_\gamma^{-1}(U_{k_i})$ и обозначим $S = \bigcup_{i=1}^n (Q_i \times H_i)$. Ясно, что S открыто в $X_\gamma \times Y_\gamma$ и $f_\gamma = \pi_\gamma \circ f \circ \iota_\gamma \in O(S)$, т. е. $h(f) = (f_\alpha | \alpha \in \Sigma) \in \Pi_\gamma^{-1}(O(S))$. Пусть теперь $g \in C_\Gamma(K, L)$, $h(g) = (g_\alpha | \alpha \in \Sigma)$ и $h(g) \in \Pi_\gamma^{-1}(O(S))$, т. е. $g_\gamma = \pi_\gamma \circ g \circ \iota_\gamma \in O(S)$. Несложно проверить, что при этом $\Gamma_g \subset \bigcup_{i=1}^n (U_{k_i} \times \pi_\gamma^{-1}(H_i)) \subset G$, т. е. $g \in O(G)$. Итак, $C_\Gamma(K, L) \xrightarrow{h} \Lambda = \varinjlim C_\Gamma(X_\alpha, Y_\alpha)$ – гомеоморфизм. Теорема доказана.

Отметим, что теоремы 5, 6 и 8 существенно усиливают аналогичные результаты, полученные в [1].

Библиографические ссылки

1. Кукрак ГО, Тимохович ВЛ, Фролова ДС. Некоторые топологические свойства функтора $C(X, Y)$. *Труды Института математики НАН Беларуси*. 2018;26(1):71–78.
2. Кукрак ГО, Тимохович ВЛ. Некоторые топологические свойства пространства отображений. *Вестник БГУ. Серия 1. Физика. Математика. Информатика*. 2010;1:144–149.
3. Тимохович ВЛ, Фролова ДС. Об инфимальной топологии пространства отображений. *Вестник БГУ. Серия 1. Физика. Математика. Информатика*. 2011;2:136–140.
4. Тимохович ВЛ, Фролова ДС. Инфимальная топология пространства отображений и отображение вычисления. *Вестник БГУ. Серия 1. Физика. Математика. Информатика*. 2012;1:68–72.
5. Тимохович ВЛ, Фролова ДС. Топологии равномерной сходимости. Собственность (в смысле Аренса – Дугунджи) и секвенциальная собственность. *Известия вузов. Математика*. 2013;9:45–58.
6. Энгелькинг Р. *Общая топология*. Москва: Мир; 1986. 752 с.
7. Bacon P. The compactness of countably compact spaces. *Pacific Journal of Mathematics*. 1970;32(3):587–592.
8. Naimpally S. Graph topology for function spaces. *Transactions of the American Mathematical Society*. 1966;123:267–272.
9. Федорчук ВВ, Филиппов ВВ. *Общая топология. Основные конструкции*. Москва: Физматлит; 2006. 336 с.
10. Букур И, Деляну А. *Введение в теорию категорий и функторов*. Райкова ДА, Ретах ВС, переводчики. Москва: Мир; 1972. 259 с.
11. Александрян РА, Мирзаханян ЭА. *Общая топология*. Москва: Высшая школа; 1979. 336 с.

References

1. Kukrak HO, Timokhovich VL, Frolova DS. [Some topological properties of the functor of $C(X, Y)$]. *Trudy Instituta matematiki NAN Belarusi*. 2018;26(1):71–78. Russian.
2. Kukrak HO, Timokhovich VL. [Some topological properties of mapping spaces]. *Vestnik BGU. Seriya 1. Fizika. Matematika. Informatika*. 2010;1:144–149. Russian.

3. Timokhovich VL, Frolova DS. [On infimal topology of mapping spaces]. *Vestnik BGU. Seriya 1. Fizika. Matematika. Informatika*. 2011;2:136–140. Russian.
4. Timokhovich VL, Frolova DS. [Infimal topology of mapping spaces and evaluation map]. *Vestnik BGU. Seriya 1. Fizika. Matematika. Informatika*. 2012;1:68–72. Russian.
5. Timokhovich VL, Frolova DS. [Topologies of uniform convergence. The property in the sense of Arens – Dugundji and the sequential property]. *Izvestiya vuzov. Matematika*. 2013;9:45–58. Russian.
6. Engelking R. *General topology*. Berkeley: John L. Keller; 1955. 298 p.
Russian edition: Engelking R. *Obshchaya topologiya*. Moscow: Mir; 1986. 752 p.
7. Bacon P. The compactness of countably compact spaces. *Pacific Journal of Mathematics*. 1970;32(3):587–592.
8. Naimpally S. Graph topology for function spaces. *Transactions of the American Mathematical Society*. 1966;123:267–272.
9. Fedorchuk VV, Filippov VV. *Obshchaya topologiya. Osnovnye konstruksii* [General topology. The main constructions]. Moscow: Fizmatlit; 2006. 336 p. Russian.
10. Bucur I, Deleanu A. *Introduction to the theory of categories and functors*. New York: NYWiley; 1968. 224 p.
Russian edition: Bucur I, Deleanu A. *Vvedenie v teoriyu kategoriy i funktorov*. Raikova DA, Retakh VS, translators. Moscow: Mir; 1972. 259 p.
11. Aleksandrian RA, Mirzakhanyan EA. *Obshchaya topologiya* [General topology]. Moscow: Vyshaya shkola; 1979. 336 p. Russian.

Статья поступила в редколлегию 27.12.2019.
Received by editorial board 27.12.2019.

ДИФФЕРЕНЦИАЛЬНЫЕ УРАВНЕНИЯ И ОПТИМАЛЬНОЕ УПРАВЛЕНИЕ

DIFFERENTIAL EQUATIONS AND OPTIMAL CONTROL

УДК 517.956.32

УСЛОВИЯ СОГЛАСОВАНИЯ ЗНАЧЕНИЙ ХАРАКТЕРИСТИЧЕСКОЙ КОСОЙ ПРОИЗВОДНОЙ НА КОНЦЕ СТРУНЫ, НАЧАЛЬНЫХ ДАННЫХ И ПРАВОЙ ЧАСТИ ВОЛНОВОГО УРАВНЕНИЯ

Е. В. УСТИЛКО¹⁾, Ф. Е. ЛОМОВЦЕВ¹⁾

¹⁾Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь

Получены достаточные условия согласования зависящих от времени характеристических первых производных в граничном режиме с начальными условиями и более общим уравнением колебаний полуограниченной струны во множествах решений всех целых высших порядков гладкости. Они обобщают найденные ранее достаточные условия согласования в случае аналогичной смешанной задачи для самого простейшего уравнения колебаний струны. Характеристичность нестационарных первых косых производных в граничном режиме означает, что в каждый момент времени они направлены вдоль критической характеристики.

Ключевые слова: смешанная задача; характеристическая первая косая производная; начальные условия; требования гладкости; условия согласования.

Образец цитирования:

Устилко ЕВ, Ломовцев ФЕ. Условия согласования значений характеристической косой производной на конце струны, начальных данных и правой части волнового уравнения. *Журнал Белорусского государственного университета. Математика. Информатика*. 2020;1:30–37. <https://doi.org/10.33581/2520-6508-2020-1-30-37>

For citation:

Ustilko EV, Lomovtsev FE. Matching conditions for values of characteristic oblique derivative at the end of a string, initial data and right-hand side of the wave equation. *Journal of the Belarusian State University. Mathematics and Informatics*. 2020; 1:30–37. Russian. <https://doi.org/10.33581/2520-6508-2020-1-30-37>

Авторы:

Екатерина Валерьевна Устилко – аспирантка кафедры математической кибернетики механико-математического факультета. Научный руководитель – Ф. Е. Ломовцев.

Фёдор Егорович Ломовцев – доктор физико-математических наук, профессор; профессор кафедры математической кибернетики механико-математического факультета.

Authors:

Ekaterina V. Ustilko, postgraduate student at the department of mathematical cybernetics, faculty of mechanics and mathematics.

ustilko@tut.by

Fiodar E. Lomovtsev, doctor of science (physics and mathematics), full professor; professor at the department of mathematical cybernetics, faculty of mechanics and mathematics.

lomovcev@bsu.by

MATCHING CONDITIONS FOR VALUES OF CHARACTERISTIC OBLIQUE DERIVATIVE AT THE END OF A STRING, INITIAL DATA AND RIGHT-HAND SIDE OF THE WAVE EQUATION

E. V. USTILKO^a, F. E. LOMOVTSSEV^a

^aBelarusian State University, 4 Niezaliežnasci Avenue, Minsk 220030, Belarus

Corresponding author: F. E. Lomovtsev (lomovtsev@bsu.by)

Sufficient matching conditions the time-dependent characteristic first derivatives in the boundary mode with the initial conditions and the more general vibration equation of a semi-bounded string are derived in the sets of solutions of all higher order smoothness orders. They generalize the previously found sufficient matching conditions in the case of a similar mixed problem for the simplest string vibration equation. The characteristic of non-stationary first oblique derivatives in the boundary mode means that at each moment of time they are directed along the critical characteristic.

Keywords: mixed problem; characteristic first oblique derivative; initial conditions; smoothness requirements; matching conditions.

Введение

В работе найдены достаточные (при завышенной на единицу гладкости решений) условия согласования нестационарных (зависящих от времени) характеристических первых производных в граничном режиме с начальными условиями и более общим ($a_1 \neq a_2$) уравнением колебаний полуограниченной струны во множествах решений всех целых высших порядков гладкости (см. постановку задачи ниже). Характеристичность этих первых производных (называемых обычно косыми производными) в граничном режиме означает, что в каждый момент времени они направлены вдоль критической характеристики уравнения [1; 2]. Найденные условия согласования обобщают выведенные ранее достаточные условия согласования в случае классических решений аналогичной смешанной задачи [3]. Вместе с требованиями гладкости правой части уравнения, начальных и граничных данных эти условия согласования нужны для гладкости решения указанной смешанной задачи на критической характеристике уравнения.

В дальнейшем полученные условия согласования будут изучены нами на необходимость, т. е. на ослабление требований гладкости, налагаемых на исходные данные (правую часть, начальные и граничные данные), до минимально достаточных. Затем их можно применить для поиска гладкого решения и установления критерия корректности по Адамару вспомогательной характеристической смешанной задачи для более общего ($a_1 \neq a_2$) уравнения колебаний полуограниченной струны во множествах решений всех целых высших порядков гладкости. Работа [4] для простейшего ($a_1 = a_2$) уравнения колебаний ограниченной струны указывает на важность условий согласования вспомогательных характеристических смешанных задач для полуограниченной струны во множествах решений всех высших порядков гладкости, потому что с увеличением значения времени возрастает гладкость всех исходных данных характеристических смешанных задач для ограниченной струны. Наконец, нами планируется использовать «метод вспомогательных смешанных задач для волнового уравнения на полупрямой» из [5], способ корректировки из [6] и эти условия согласования для нахождения устойчивого по правой части уравнения, начальным и граничным данным единственного классического решения смешанной задачи для более общего ($a_1 \neq a_2$) уравнения колебаний ограниченной струны при нестационарных характеристических первых косых производных на ее концах. Указанный метод позволяет выводить в явном виде классические решения и критерии корректности смешанных задач для уравнений колебаний ограниченной струны без продолжений исходных данных задач вне множеств их изначального задания для гиперболических уравнений [7–9], а его аналог – для нестрогих гиперболических уравнений [10; 11].

Постановка задачи поиска достаточных условий согласования

На множестве $\dot{G}_\infty =]0, +\infty[\times]0, +\infty[$ рассматривается характеристическая смешанная задача

$$u_{tt}(x, t) + (a_1 - a_2)u_{xt}(x, t) - a_1 a_2 u_{xx}(x, t) = f(x, t), (x, t) \in \dot{G}_\infty, \quad (1)$$

$$u|_{t=0} = \varphi(x), \quad \partial_t u|_{t=0} = \psi(x), \quad x \in]0, +\infty[, \quad (2)$$

$$\alpha(t)u_t(x, t) + \beta(t)u_x(x, t) + \gamma(t)u(x, t)|_{x=0} = \mu(t), t \in]0, +\infty[, \quad (3)$$

где коэффициенты уравнения $a_1 > 0$, $a_2 > 0$ – вещественные постоянные; коэффициенты граничного режима $\alpha(t)$, $\beta(t) = a_1\alpha(t)$, $\gamma(t) \neq 0$ – заданные функции переменной t ; исходные данные задачи f , φ , ψ , μ – заданные функции своих переменных x и t .

На основе физической интерпретации общего интеграла доказывается так же, как в [1, с. 54–59], что уравнение (1) моделирует вынужденные колебания однородной струны. Эти колебания представляют собой результат наложения прямой и обратной волн, движущихся соответственно в положительном и отрицательном направлениях оси Ox со скоростями a_1 и a_2 , и воздействия вынуждающей силы с плотностью f . Если $a_1 = a_2$, то струна колеблется в покоящейся среде, не оказывающей сопротивления, и тогда уравнение (1) – общеизвестное уравнение колебаний однородной среды. Если же $a_1 \neq a_2$, то струна колеблется в движущейся, упруго сопротивляющейся однородной среде.

Пусть $C(\Omega)$ – множество непрерывных функций на подмножестве Ω плоскости $\mathbb{R}^2$, $C^k(\Omega)$ – множество всех k раз непрерывно дифференцируемых функций на Ω , $k \in \mathbb{N}$, $k \geq 2$.

Уравнение (1) в плоскости $\mathbb{R}^2$ переменных x и t имеет два различных семейства характеристик: $x - a_1t = C_1$, $x + a_2t = C_2$, $C_1, C_2 \in \mathbb{R} =]-\infty, +\infty[$.

Первая четверть плоскости $G_\infty = [0, +\infty[\times [0, +\infty[$ разбивается характеристикой $x = a_1t$ на два множества: $G_- = \{(x, t) \in G_\infty : x > a_1t, t \geq 0\}$ и $G_+ = \{(x, t) \in G_\infty : x \leq a_1t, x \geq 0\}$. В процессе решения аналогичной смешанной задачи для уравнения колебаний ограниченной струны при характеристических и нестационарных первых косых производных на ее концах во множестве классических решений $C^2(G_\infty)$ возникает потребность в решении вспомогательной характеристической смешанной задачи (1)–(3) для уравнения колебаний полуограниченной струны во множествах гладких решений $C^m(G_\infty)$, $m \geq 2$. Согласно алгоритму нахождения единственного и устойчивого по исходным данным f , φ , ψ , μ решения этой вспомогательной задачи сначала ищут решение u_- задачи Коши (1), (2) в G_- , затем решение u_+ соответствующей задачи Пикара в G_+ и с помощью необходимых и достаточных требований гладкости и условий согласования доказывают m раз непрерывную дифференцируемость функций u_- , u_+ на $x = a_1t$. В настоящей работе требуется найти только достаточные условия согласования граничного режима (3) с начальными условиями (2) и уравнением (1) на $x = a_1t$ для более гладких решений из $C^{m+1}(G_\infty)$, $m \geq 2$.

Вывод достаточных условий согласования

Для более гладких решений $u \in C^{m+1}(G_\infty)$ смешанной задачи (1)–(3) из уравнения (1), начальных условий (2) и граничного режима (3) вытекают очевидные требования гладкости исходных данных:

$$f \in C^{m-1}(G_\infty), \varphi \in C^{m+1}[0, +\infty[, \psi \in C^m[0, +\infty[, \mu \in C^m[0, +\infty[. \quad (4)$$

Полагая $t = 0$ в режиме (3) и первой производной по t от этого режима и вычисляя значения слагаемых их левых частей с помощью начальных условий (2) при $x = 0$ и уравнения (1) при $t = 0$, $x = 0$, получаем для классических решений этой задачи два первых достаточных условия согласования начальных и граничных данных и правой части уравнения:

$$\alpha(0)(\psi(0) + a_1\varphi'(0)) + \gamma(0)\varphi(0) = \mu(0), \quad (5)$$

$$\alpha'(0)(\psi(0) + a_1\varphi'(0)) + \gamma'(0)\varphi(0) + \alpha(0)(a_2(\psi'(0) + a_1\varphi''(0)) + f(0, 0)) + \gamma(0)\psi(0) = \mu'(0). \quad (6)$$

Справедливо следующее утверждение.

Утверждение. Пусть в граничном режиме (3) с коэффициентами $\alpha, \beta, \gamma \in C^m(\mathbb{R}_+)$ косая производная является характеристической, т. е. $a_1\alpha(t) = \beta(t)$, $\gamma(t) \neq 0$, $t \in \mathbb{R}_+ = [0, +\infty[$. Если существует решение $u \in C^{m+1}(G_\infty)$ смешанной задачи (1)–(3), то для $f \in C^{m-1}(G_\infty)$, $\varphi \in C^{m+1}(\mathbb{R}_+)$, $\psi \in C^m(\mathbb{R}_+)$, $\mu \in C^m(\mathbb{R}_+)$ из (4) верны условия согласования (5), (6) и справедливо

$$\begin{aligned}
 & \alpha^{(q)}(0)(\psi(0) + a_1\varphi'(0)) + \gamma^{(q)}(0)\varphi(0) + \\
 & + q\left(\alpha^{(q-1)}(0)(a_2(\psi'(0) + a_1\varphi''(0)) + f(0, 0)) + \gamma^{(q-1)}(0)\psi(0)\right) + \\
 & + \sum_{i=2}^q C_q^i \left(\alpha^{(q-i)}(0) \left(a_2^i (\psi^{(i)}(0) + a_1\varphi^{(i+1)}(0)) + \sum_{j=0}^{i-1} a_2^j f^{(j; i-j-1)}(0, 0) \right) + \right. \\
 & \quad \left. + \gamma^{(q-i)}(0) \left(a_2 \frac{a_2^{i-1} - (-a_1)^{i-1}}{a_1 + a_2} (\psi^{(i-1)}(0) + a_1\varphi^{(i)}(0)) + \right. \right. \\
 & \quad \left. \left. + \sum_{k=0}^{i-1} \frac{a_2^{k+1} - (-a_1)^{k+1}}{a_1 + a_2} f^{(k; i-k-2)}(0, 0) + (-a_1)^{i-1} \psi^{(i-1)}(0) \right) \right) = \mu^{(q)}(0), \quad q = 2, 3, \dots, m. \quad (7)
 \end{aligned}$$

Доказательство. Введем обозначение $\frac{\partial^{k+l} u(x, t)}{\partial x^k \partial t^l} = u^{(k; l)}(x, t)$. Тогда, учитывая характеристичность режима (3), т. е. $\beta(t) = a_1 \alpha(t)$, $t \in \mathbb{R}_+$, его можно записать в виде

$$\left(\alpha(t) \left(u^{(0; 1)}(x, t) + a_1 u^{(1; 0)}(x, t) \right) + \gamma(t) u(x, t) \right) \Big|_{x=0} = \mu(t), \quad t \in \mathbb{R}_+. \quad (8)$$

Продифференцируем q раз граничный режим (8) по переменной t :

$$\sum_{i=0}^q C_q^i \left(\alpha^{(q-i)}(t) \left[u^{(0; i+1)}(x, t) + a_1 u^{(1; i)}(x, t) \right] + \gamma^{(q-i)}(t) u^{(0; i)}(x, t) \right) \Big|_{x=0} = \mu^{(q)}(t), \quad (9)$$

где $C_q^i = \frac{q!}{i!(q-i)!}$, $q \geq 2$. Непосредственно из уравнения (1) следует равенство

$$\begin{aligned}
 u^{(0; 2)}(x, t) &= a_1 a_2 u^{(2; 0)}(x, t) + (a_2 - a_1) u^{(1; 1)}(x, t) + f(x, t) = \\
 &= a_2 \left(u^{(1; 1)}(x, t) + a_1 u^{(2; 0)}(x, t) \right) - a_1 u^{(1; 1)}(x, t) + f(x, t).
 \end{aligned}$$

Дифференцируем это равенство l раз по переменной x и $n-2$ раза по переменной t :

$$u^{(l; n)}(x, t) = a_2 \left(u^{(l+1; n-1)}(x, t) + a_1 u^{(l+2; n-2)}(x, t) \right) - a_1 u^{(l+1; n-1)}(x, t) + f^{(l; n-2)}(x, t), \quad n \geq 2. \quad (10)$$

В выражении в квадратных скобках из (9) запишем производную $u^{(0; i+1)}(x, t)$, используя формулу (10) при $l=0$, $n=i+1$:

$$\begin{aligned}
 u^{(0; i+1)}(x, t) + a_1 u^{(1; i)}(x, t) &= a_2 \left(u^{(1; i)}(x, t) + a_1 u^{(2; i-1)}(x, t) \right) - a_1 u^{(1; i)}(x, t) + \\
 + f^{(0; i-1)}(x, t) + a_1 u^{(1; i)}(x, t) &= a_2 \left(u^{(1; i)}(x, t) + a_1 u^{(2; i-1)}(x, t) \right) + f^{(0; i-1)}(x, t). \quad (11)
 \end{aligned}$$

Можно заметить, что по сравнению с левой частью равенства (11) в его правой части порядок производных от функции u по переменной t снизился на единицу, а порядок производных по переменной x повысился на единицу. Более того, она записана в виде $u^{(1; i)}(x, t) + a_1 u^{(2; i-1)}(x, t)$, аналогичном виду исходного выражения $u^{(0; i+1)}(x, t) + a_1 u^{(1; i)}(x, t)$, $i = \overline{1, q}$. Поэтому и далее будем пользоваться формулами (10) и (11) так, чтобы положительный порядок производных по переменной t от функции u стал не выше 1.

На первом шаге этого процесса с помощью формулы (10) при $l=1$, $n=i$ имеем равенство

$$\begin{aligned}
 & a_2 \left(u^{(1; i)}(x, t) + a_1 u^{(2; i-1)}(x, t) \right) + f^{(0; i-1)}(x, t) = \\
 & = a_2^2 \left(u^{(2; i-1)}(x, t) + a_1 u^{(3; i-2)}(x, t) \right) + a_2 f^{(1; i-2)}(x, t) + f^{(0; i-1)}(x, t),
 \end{aligned}$$

аналогичное равенству (11). На втором шаге из формулы (10) при $l = 2, n = i - 1$ находим

$$\begin{aligned} & a_2^2 \left(u^{(2;i-1)}(x, t) + a_1 u^{(3;i-2)}(x, t) \right) + a_2 f^{(1;i-2)}(x, t) + f^{(0;i-1)}(x, t) = \\ & = a_2^3 \left(u^{(3;i-2)}(x, t) + a_1 u^{(4;i-3)}(x, t) \right) + a_2^2 f^{(2;i-3)}(x, t) + a_2 f^{(1;i-2)}(x, t) + f^{(0;i-1)}(x, t). \end{aligned}$$

После i -го шага при $l = i - 1, n = 2$ приходим к формуле

$$u^{(0;i+1)}(x, t) + a_1 u^{(1;i)}(x, t) = a_2^i \left(u^{(i;1)}(x, t) + a_1 u^{(i+1;0)}(x, t) \right) + \sum_{j=0}^{i-1} a_2^j f^{(j;i-j-1)}(x, t), \quad i \geq 1. \quad (12)$$

В равенстве (9) осталось преобразовать слагаемое $u^{(0;i)}(x, t), i = \overline{2, q}$. Верны следующие соотношения:

$$\begin{aligned} & u^{(0;i)}(x, t) = u^{(0;i)}(x, t) + a_1 u^{(1;i-1)}(x, t) - a_1 u^{(1;i-1)}(x, t) = \\ & = u^{(0;i)}(x, t) + a_1 u^{(1;i-1)}(x, t) - a_1 \left(u^{(1;i-1)}(x, t) + a_1 u^{(2;i-2)}(x, t) \right) + a_1^2 u^{(2;i-2)}(x, t) = \\ & = \sum_{k=0}^{i-2} (-a_1)^k \left[u^{(k;i-k)}(x, t) + a_1 u^{(k+1;i-k-1)}(x, t) \right] + (-a_1)^{i-1} u^{(i-1;1)}(x, t). \end{aligned} \quad (13)$$

Продифференцируем l раз по x равенство (12) при $i = n - 1$ и получим представления

$$\begin{aligned} & u^{(l;n)}(x, t) + a_1 u^{(l+1;n-1)}(x, t) = \\ & = a_2^{n-1} \left(u^{(l+n-1;1)}(x, t) + a_1 u^{(l+n;0)}(x, t) \right) + \sum_{j=0}^{n-2} a_2^j f^{(l+j;n-j-2)}(x, t), \quad n \geq 2. \end{aligned} \quad (14)$$

Для выражения в квадратных скобках из (13) применим формулу (14) при $l = k, n = i - k$. Тогда частная производная $u^{(0;i)}(x, t)$ равна функции

$$\sum_{k=0}^{i-2} (-a_1)^k \left(a_2^{i-k-1} \left[u^{(i-1;1)}(x, t) + a_1 u^{(i;0)}(x, t) \right] + \sum_{j=0}^{i-k-2} a_2^j f^{(k+j;i-k-j-2)}(x, t) \right) + (-a_1)^{i-1} u^{(i-1;1)}(x, t).$$

Поскольку слагаемые в квадратных скобках не зависят от индекса k , то эту функцию можно записать как

$$\begin{aligned} & \left(u^{(i-1;1)}(x, t) + a_1 u^{(i;0)}(x, t) \right) \sum_{k=0}^{i-2} (-a_1)^k a_2^{i-k-1} + \\ & + \sum_{k=0}^{i-2} (-a_1)^k \sum_{j=0}^{i-k-2} a_2^j f^{(k+j;i-k-j-2)}(x, t) + (-a_1)^{i-1} u^{(i-1;1)}(x, t). \end{aligned}$$

Воспользуемся очевидными равенствами

$$\sum_{k=0}^{i-2} (-a_1)^k a_2^{i-k-2} = a_2^{i-2} - a_1 a_2^{i-3} + a_1^2 a_2^{i-4} - \dots + (-a_1)^{i-2} = \frac{a_2^{i-1} - (-a_1)^{i-1}}{a_1 + a_2}, \quad (15)$$

$$\begin{aligned} & \sum_{k=0}^{i-2} (-a_1)^k \sum_{j=0}^{i-k-2} a_2^j f^{(k+j;i-k-j-2)}(x, t) = \\ & = \sum_{s=0}^{i-2} f^{(s;i-s-2)}(x, t) \sum_{v=0}^s (-a_1)^v a_2^{s-v} = \sum_{s=0}^{i-2} \frac{a_2^{s+1} - (-a_1)^{s+1}}{a_1 + a_2} f^{(s;i-s-2)}(x, t) \end{aligned}$$

и придем к формуле

$$u^{(0;i)}(x, t) = a_2 \frac{a_2^{i-1} - (-a_1)^{i-1}}{a_1 + a_2} \left(u^{(i-1;1)}(x, t) + a_1 u^{(i;0)}(x, t) \right) + \\ + \sum_{s=0}^{i-2} \frac{a_2^{s+1} - (-a_1)^{s+1}}{a_1 + a_2} f^{(s; i-s-2)}(x, t) + (-a_1)^{i-1} u^{(i-1;1)}(x, t). \quad (16)$$

Здесь во второй строке равенств (15) мы сначала в соответствующей сумме меняем индекс $s = k + j$, потом суммируем коэффициенты при одинаковых частных производных от f и, наконец, находим значения числовых сумм с помощью первой строки этих равенств.

В левой части (9) к слагаемым суммы для $i \geq 2$ применим формулы (12) и (16) и получим

$$\left(\alpha^{(q)}(t) \left(u^{(0;1)}(x, t) + a_1 u^{(1;0)}(x, t) \right) + \gamma^{(q)}(t) u(x, t) \right) + \\ + q \left(\alpha^{(q-1)}(t) \left(u^{(0;2)}(x, t) + a_1 u^{(1;1)}(x, t) \right) + \gamma^{(q-1)}(t) u^{(0;1)}(x, t) \right) + \\ + \sum_{i=2}^q C_q^i \left(\alpha^{(q-i)}(t) \left(a_2^i \left(u^{(i;1)}(x, t) + a_1 u^{(i+1;0)}(x, t) \right) + \sum_{j=0}^{i-1} a_2^j f^{(j; i-j-1)}(x, t) \right) + \right. \\ \left. + \gamma^{(q-i)}(t) \left(a_2 \frac{a_2^{i-1} - (-a_1)^{i-1}}{a_1 + a_2} \left(u^{(i-1;1)}(x, t) + a_1 u^{(i;0)}(x, t) \right) + \right. \\ \left. \left. + \sum_{k=0}^{i-2} \frac{a_2^{k+1} - (-a_1)^{k+1}}{a_1 + a_2} f^{(k; i-k-2)}(x, t) + (-a_1)^{i-1} u^{(i-1;1)}(x, t) \right) \right) \Bigg|_{x=0} = \mu^{(q)}(t), \quad q \geq 2. \quad (17)$$

В силу представления (14) при $l = 0$, $n = 2$ справедливо преобразование

$$u^{(0;2)}(x, t) + a_1 u^{(1;1)}(x, t) = a_2 \left(u^{(1;1)}(x, t) + a_1 u^{(2;0)}(x, t) \right) + f(x, t).$$

Если в (17) воспользоваться этим преобразованием, положить $t = 0$ и учесть начальные условия (2), то будем иметь условия согласования (7).

Замечание. Условия согласования (7) при $q = 0$ и $q = 1$, очевидно, становятся условиями согласования (5) и (6) соответственно. Для функций $u \in C^m(G_\infty)$ условие (7) при $q = m$ определено для $\varphi \in C^{m+1}(\mathbb{R}_+)$, $\psi, \mu \in C^m(\mathbb{R}_+)$, $f \in C^{m-1}(G_\infty)$ и является лишь достаточным, потому что для $u \in C^m(G_\infty)$ эти исходные данные – только $\varphi(x) = u(x, 0) \in C^m(\mathbb{R}_+)$, $\psi(0) = u_t(x, 0) \in C^{m-1}(\mathbb{R}_+)$, $f(x, t) = u_{tt}(x, t) + (a_1 - a_2)u_{xt}(x, t) - a_1 a_2 u_{xx}(x, t) \in C^{m-2}(G_\infty)$. Для существования слагаемых левой части равенства (7) при $q = m$ не нужна завышенная гладкость $u \in C^{m+1}(G_\infty)$, но хватает минимальной (необходимой) гладкости, а именно $\alpha(0)\varphi^{(m+1)}(0)$, $\alpha(0)\psi^{(m)}(0) \in \mathbb{R}_+$ и существования произведения $\alpha(0)$ и производной по вектору $\vec{v} = (a_2, 1)$ от соответствующей суммы частных производных порядка $m - 2$ от правой части f в начале координат $(0, 0)$.

Необходимость этих и более общих требований гладкости для решений $u \in C^m(G_\infty)$ будет строго доказана модификацией метода характеристик [1] в наших следующих исследованиях. В дальнейшем необходимость условий согласования типа (7) характеристической смешанной задачи для решений $u \in C^m(G_\infty)$, $m \geq 2$, получится предельным переходом с гладких функций $u \in C^{m+1}(G_\infty)$ на данные f, φ, ψ, μ с минимально возможной их гладкостью. При $m = 2$ это уже сделано в работе [3]. В случае $a_1 = a_2 = a > 0$ и гладкости исходных данных f, φ, ψ, μ , указанной в утверждении, условия согласования (7) совпадают с условиями согласования из критерия корректности вспомогательной смешанной задачи для полуограниченной струны, который использован в [4].

Заклучение

В настоящей работе выведены достаточные условия согласования характеристических нестационарных первых производных на конце полуограниченной струны с начальными условиями и более общим одномерным волновым уравнением для решений $u \in C^{m+1}(G_\infty)$, $m \geq 2$, этой смешанной задачи. Указанные условия очевидно обеспечивают m раз непрерывную дифференцируемость решения u на критической характеристике $x = a_1 t$ уравнения. В дальнейшем полученные достаточные условия согласования (5)–(7) будут ослаблены до необходимых и использованы для явного вычисления единственного и устойчивого по f , φ , ψ , μ классического решения и вывода критерия корректности по Адамару аналогичной вспомогательной смешанной задачи во множестве решений, принадлежащих $C^m(G_\infty)$, $m \geq 2$.

Библиографические ссылки

1. Тихонов АН, Самарский АА. *Уравнения математической физики*. Москва: Наука; 2004. 798 с.
2. Барановская СН, Юрчук НИ. Смешанная задача для уравнения колебания струны с зависящей от времени косой производной в краевом условии. *Дифференциальные уравнения*. 2009;45(8):1188–1191.
3. Ломовцев ФЕ, Устилко ЕВ. Критерий корректности смешанной задачи для общего уравнения колебаний полуограниченной струны с нестационарной характеристической первой косой производной в граничном условии. *Вестник Віцебскага дзяржаўнага ўніверсітэта*. 2018;4(101):18–28.
4. Ломовцев ФЕ, Точко ТС. Смешанная задача для неоднородного уравнения колебаний ограниченной струны при характеристических нестационарных первых косых производных на концах. *Вестник Гродзенскага дзяржаўнага ўніверсітэта імя Янкі Купалы. Серыя 2. Матэматыка. Фізіка. Інфарматыка, вылічальна тэхніка і кіраванне*. 2019;9(2):56–75.
5. Ломовцев ФЕ. Метод вспомогательных смешанных задач для полуограниченной струны. В: *Шестые Богдановские чтения по обыкновенным дифференциальным уравнениям. Материалы Международной математической конференции; 7–10 декабря 2015 г.; Минск, Беларусь. Часть 2*. Минск: Институт математики НАН Беларуси; 2015. с. 74–75.
6. Ломовцев ФЕ. Метод корректировки пробных решений общего волнового уравнения в первой четверти плоскости для минимальной гладкости его правой части. *Журнал Белорусского государственного университета. Математика. Информатика*. 2017;3:38–52.
7. Ломовцев ФЕ. Решение без продолжения данных смешанной задачи для неоднородного уравнения колебаний струны при граничных косых производных. *Дифференциальные уравнения*. 2016;52(8):1128–1132.
8. Ломовцев ФЕ. Необходимые и достаточные условия вынужденных колебаний полуограниченной струны с первой характеристической косой производной в нестационарном граничном условии. *Весті Нацыянальнай акадэміі навук Беларусі. Серыя фізіка-матэматычных навук*. 2016;1:21–27.
9. Новиков ЕН. Смешанные задачи для уравнения вынужденных колебаний ограниченной струны при нестационарных граничных условиях с первой и второй косыми производными [диссертация]. Минск: БГУ; 2017. 258 с.
10. Ломовцев ФЕ, Юрчук НИ. Решение начально-краевой задачи для нестрого гиперболического уравнения при смешанных граничных условиях в четверти плоскости. *Весті Нацыянальнай акадэміі навук Беларусі. Серыя фізіка-матэматычных навук*. 2016;3:51–57.
11. Ломовцев ФЕ. Критерий корректности смешанной задачи для одного параболического уравнения на отрезке со смешанными граничными условиями на концах. В: *Современные методы теории функций и смежные проблемы. Воронежская зимняя математическая школа. Материалы международной конференции; 28 января – 2 февраля 2019 г.; Воронеж, Россия*. Воронеж: Издательский дом ВГУ; 2019. с. 184–185.

References

1. Tikhonov AN, Samarskiy AA. *Uravneniya matematicheskoi fiziki* [The equations of mathematical physics]. Moscow: Nauka; 2004. 798 p. Russian.
2. Baranovskaya SN, Yurchuk NI. [Mixed problem for the oscillation equation of a string with a time-dependent oblique derivative in the boundary condition]. *Differentsial'nye uravneniya*. 2009;45(8):1188–1191. Russian.
3. Lomovtsev FE, Ustilko EV. Correctness criterion of a mixed problem for the general oscillations equation of a semi-bounded string with a non-stationary characteristic of first directional derivative in a boundary condition. *Vesnik Vicebskaga dzjarzhawnaga wniversitjeta*. 2018;4(101):18–28. Russian.
4. Lomovtsev FE, Tochko TS. [Mixed problem for the inhomogeneous equation of oscillations of a bounded string for characteristic unsteady first oblique derivatives at the ends]. *Vesnik Grodzenskaga dzjarzhawnaga wniversitjeta imja Janki Kupaly. Serija 2. Matjematyka. Fizika. Infarmatyka, vylichal'naja tjehnika i kiravanne*. 2019;9(2):56–75. Russian.
5. Lomovtsev FE. [The method of auxiliary mixed problems for a semi-bounded string]. In: *Shesty Bogdanovskie chteniya po obyknovennym differentsial'nyim uravneniyam. Materialy Mezhduнародnoi matematicheskoi konferentsii; 7–10 dekabrya 2015 g.; Minsk, Belarus'. Chast' 2* [The sixth Bogdanov readings on ordinary differential equations. Proceedings of the International mathematical conference; 2015 December 7–10; Minsk, Belarus. Part 2]. Minsk: Institute of Mathematics, National Academy of Sciences of Belarus; 2015. p. 74–75. Russian.
6. Lomautsau FE. Correction method of test solutions of the general wave equation in the first quarter of the plane for minimal smoothness of its right-hand side. *Journal of the Belarusian State University. Mathematics and Informatics*. 2017;3:38–52. Russian.
7. Lomovtsev FE. [Solution without extension of the data of the mixed problem for the inhomogeneous oscillation equation of a string with boundary oblique derivatives]. *Differentsial'nye uravneniya*. 2016;52(8):1128–1132. Russian.

8. Lomovtsev FE. Necessary and sufficient conditions for forced vibrations of a semibounded string with the first characteristic directional derivative in the unsteady boundary condition. *Proceedings of the National Academy of Sciences of Belarus. Physics and Mathematics Series*. 2016;1:21–27. Russian.

9. Novikov EN. [Mixed problems for the equation of forced oscillations of a bounded string under non-stationary boundary conditions with first and second oblique derivatives] [dissertation]. Minsk: Belarusian State University; 2017. 258 p. Russian.

10. Lomovtsev FE, Yurchuk NI. Initial boundary value problem for the non-strictly hyperbolic equation with mixed boundary conditions in a quadrant. *Proceedings of the National Academy of Sciences of Belarus. Physics and Mathematics Series*. 2016;3:51–57. Russian.

11. Lomovtsev FE. [Correctness criterion of the mixed problem for one parabolic equation on an interval with mixed boundary conditions at the ends]. In: *Sovremennye metody teorii funktsii i smezhnye problemy. Voronezhskaya zimnyaya matematicheskaya shkola. Materialy mezhdunarodnoi konferentsii; 28 yanvarya – 2 fevralya 2019 g.; Voronezh, Rossiya* [Voronezh Winter Mathematical School. Proceedings of the International conference; 2019 January 28 – February 2; Voronezh, Russia]. Voronezh: Voronezh State University Publishing House; 2019. p. 184–185. Russian.

Статья поступила в редколлегию 03.06.2019.
Received by editorial board 03.06.2019.

ТЕОРЕТИЧЕСКАЯ И ПРИКЛАДНАЯ МЕХАНИКА

THEORETICAL AND PRACTICAL MECHANICS

УДК 539.3,519.6

ВЛИЯНИЕ УСЛОВИЙ ЗАКРЕПЛЕНИЯ НА ПОЯВЛЕНИЕ НЕСИММЕТРИЧНЫХ ФОРМ РАВНОВЕСИЯ У КРУГЛЫХ ПЛАСТИН ПОД ДЕЙСТВИЕМ НОРМАЛЬНОГО ДАВЛЕНИЯ

С. М. БАУЭР^{1), 2)}, Е. Б. ВОРОНКОВА^{1), 2)}

¹⁾Санкт-Петербургский государственный университет,
Университетская набережная, 7/9, 199034, г. Санкт-Петербург, Россия

²⁾Научно-образовательный центр «Материалы»
Донского государственного технического университета,
пл. Гагарина, 1, 344000, г. Ростов-на-Дону, Россия

Рассматривается устойчивость осесимметричных форм равновесия неоднородных круглых пластин, нагруженных нормальным давлением, с упруго закрепленным краем. В предположении, что несимметричная составляющая решения носит периодический характер, численным методом определяется наименьшее значение нагрузки,

Образец цитирования:

Бауэр СМ, Воронкова ЕБ. Влияние условий закрепления на появление несимметричных форм равновесия у круглых пластин под действием нормального давления. *Журнал Белорусского государственного университета. Математика. Информатика*. 2020;1:38–46.
<https://doi.org/10.33581/2520-6508-2020-1-38-46>

For citation:

Bauer SM, Voronkova EB. Influence of boundary constraints on the appearance of asymmetrical equilibrium states in circular plates under normal pressure. *Journal of the Belarusian State University. Mathematics and Informatics*. 2020;1:38–46. Russian.
<https://doi.org/10.33581/2520-6508-2020-1-38-46>

Авторы:

Светлана Михайловна Бауэр – доктор физико-математических наук, профессор; профессор кафедры теоретической и прикладной механики математико-механического факультета¹⁾, ведущий исследователь лаборатории механики биосовместимых материалов²⁾.

Ева Боруховна Воронкова – кандидат физико-математических наук; доцент кафедры математического моделирования энергетических систем факультета прикладной математики – процессов управления¹⁾, младший научный сотрудник лаборатории механики биосовместимых материалов²⁾.

Authors:

Svetlana M. Bauer, doctor of science (physics and mathematics), full professor; professor at the department of theoretical and applied mechanics, faculty of mathematics and mechanics^a, and leading researcher at the laboratory of mechanics of biomaterials^b.

s.bauer@spbu.ru

<https://orcid.org/0000-0003-3732-2110>

Eva B. Voronkova, PhD (physics and mathematics); associate professor at the department of mathematical modeling of power systems, faculty of applied mathematics and control processes^a, and junior researcher at the laboratory of mechanics of biomaterials^b.

e.voronkova@spbu.ru

<https://orcid.org/0000-0002-3065-4473>

при которой происходит бифуркация в несимметричное состояние. Исследовано влияние степени неоднородности материала и условий закрепления края на величину критической нагрузки и форму потери устойчивости. Показано, что с увеличением жесткости пружины, препятствующей свободному смещению края пластины в радиальном направлении, бифуркация в несимметричное состояние может происходить при существенно больших нагрузках и с образованием большего числа волн в окружном направлении. Уменьшение жесткости оболочки к краю приводит к значительному снижению величины критической нагрузки, если радиальные перемещения края пластины ничем не ограничены.

Ключевые слова: круглая пластина; потеря устойчивости; неоднородность.

Благодарность. Работа выполнена при финансовой поддержке Правительства Российской Федерации (грант № 14.Z50.31.0046).

INFLUENCE OF BOUNDARY CONSTRAINTS ON THE APPEARANCE OF ASYMMETRICAL EQUILIBRIUM STATES IN CIRCULAR PLATES UNDER NORMAL PRESSURE

S. M. BAUER^{a, b}, E. B. VORONKOVA^{a, b}

^a*Saint Petersburg State University, 7/9 Universitetskaya Embankment,
Saint Petersburg 199034, Russia*

^b*Research and Education Center «Materials», Don State Technical University,
1 Gagarina Square, Rostov-on-Don 344000, Russia*

Corresponding author: E. B. Voronkova (e.voronkova@spbu.ru)

Unsymmetrical buckling of nonuniform circular plates with elastically restrained edge and subjected to normal pressure is studied in this paper. The unsymmetric part of the solution is sought in terms of multiples of the harmonics of the angular coordinate. A numerical method is employed to obtain the lowest load value, which leads to the appearance of waves in the circumferential direction. The effect of material heterogeneity and boundary on the buckling load is examined. It is shown that if the outer edge of a plate is elastically restrained against radial deflection, the buckling load for unsymmetrical buckling is larger than for a plate with a movable edge. The elasticity modulus decrease away from the center of a plate leads to sufficient lowering of the buckling pressure if the outer edge can move freely in the radial direction.

Keywords: circular plate; buckling; heterogeneity.

Acknowledgements. This research was supported by the Government of Russia (grant No. 14.Z50.31.0046).

Введение

Появлению неосесимметричных форм равновесия у сферических, тороидальных, эллипсоидальных оболочек, нагруженных нормальным внутренним давлением, посвящено множество работ [1–4]. При этом отмечается, что точность описания докритического состояния может существенно повлиять на вычисление значений критической нагрузки и формы потери устойчивости [2; 5].

Д. Ю. Панов и В. И. Феодосьев первыми предложили решение, соответствующее несимметричным формам равновесия круглой пластины, загруженной нормально распределенным давлением [3].

Они аппроксимировали неосесимметричный нормальный прогиб пластины выражением вида $w(r, \theta) =$

$$= \left(1 - \left(\frac{r}{R}\right)^2\right)^2 \left(A + B\left(\frac{r}{R}\right)^4 \cos n\theta\right), \text{ где } r, \theta - \text{координаты срединной поверхности пластины } 0 \leq r \leq R,$$

$0 \leq \theta \leq 2\pi$; A, B – неизвестные константы, $n \geq 2$, и, используя метод Галёркина, нашли минимальное значение нагрузки и волновое число n , соответствующие появлению волн по краю пластины. Однако позже именно В. И. Феодосьевым было показано, что использования одного или двух параметров для описания докритического состояния пластины или оболочки недостаточно [5]. Доказательство существования решения, соответствующего несимметричным формам равновесия у симметрично загруженной пластины, проведено Н. Ф. Морозовым [6], единственность такого решения доказана В. О. Писечки [7].

Л. С. Чео и Е. Л. Райсс численно определили значения критической нагрузки, при которой круглая пластина теряет устойчивость осесимметричных форм равновесия [8]. Сопоставляя свои решения с результатами Д. Ю. Панова и В. И. Феодосьева, авторы [8] также подчеркивают, что аппроксимация неосесимметричного решения, принятая в [3], недостаточно точно описывает устойчивое закритическое состояние равновесия.

Сравнение значений критической нагрузки, при которой пластина переходит в неосесимметричное состояние равновесия, найденных численным и асимптотическим методом, проведено в работах [9; 10]. Аналитические модели для описания краевого несимметричного выпучивания круглой пластины при равномерном нагреве и сравнение с экспериментальными данными представлены в [11]. Задача о потере устойчивости симметричных форм равновесия круглой или кольцевой пластиной, модуль упругости которой изменяется при движении от центра пластины к ее краю, рассматривалась в [12]. В работе [13] исследована бифуркация в несимметричное состояние пологой сферической оболочки, нагруженной внутренним давлением. Роль граничных условий в появлении несимметричных форм равновесия у полой оболочки затронута в [10].

В настоящей работе обсуждается влияние условий закрепления на появление несимметричных форм равновесия у неоднородной круглой пластины.

Материалы и методы исследования

Постановка задачи. Рассмотрим круглую изотропную пластину, находящуюся под действием равномерно распределенного нормального давления. Считая, что модуль упругости пластины изменяется при удалении от центра пластины к ее краю, запишем разрешающую систему уравнений в виде [12; 13]

$$\begin{aligned} D\Delta\Delta w + \frac{\partial D}{\partial r}L_1^+(w) + \frac{\partial^2 D}{\partial r^2}L_2^+(w) &= p + L(w, F), \\ \frac{\Delta\Delta F}{E} + \frac{\partial}{\partial r}\left(\frac{1}{E}\right)L_1^-(F) + \frac{\partial^2}{\partial r^2}\left(\frac{1}{E}\right)L_2^-(F) &= -\frac{h}{2}L(w, w), \end{aligned} \quad (1)$$

где $w = w(r, \theta)$, $F = F(r, \theta)$ – искомые функция нормального прогиба и функция усилий соответственно, r, θ – введенные полярные координаты срединной поверхности пластины ($0 \leq r \leq R$, $0 \leq \theta \leq 2\pi$);

$D = D(r) = \frac{E(r)}{12(1-\nu^2)}$ – цилиндрическая жесткость пластины, ν – коэффициент Пуассона материала

пластины; $E = E(r)$ – модуль упругости пластины, зависящий от радиальной координаты; p – нормальное давление, действующее на пластину; h – толщина пластины; оператор Лапласа Δ и дифференциальные операторы $L, L_i^\pm$ ($i = 1, 2$) имеют вид

$$\begin{aligned} \Delta &= \left(\frac{\partial}{\partial r}\right)^2 + \frac{1}{r}\frac{\partial}{\partial r} + \frac{1}{r^2}\frac{\partial^2}{\partial \theta^2}, \\ L(x, y) &= x''\left(\frac{y'}{r} + \frac{\ddot{y}}{r^2}\right) + y''\left(\frac{x'}{r} + \frac{\ddot{x}}{r^2}\right) - 2\left(\frac{\dot{x}'}{r} - \frac{\dot{x}}{r^2}\right)\left(\frac{\dot{y}'}{r} - \frac{\dot{y}}{r^2}\right), \\ L_1^\pm(y) &= 2y''' + \frac{2 \pm \nu}{r}y'' + \frac{2}{r^2}(\ddot{y})' - \frac{y'}{r^2} - 3\frac{\ddot{y}}{r^3}, \\ L_2^\pm(y) &= y'' \pm \nu\left(\frac{y'}{r} + \frac{\ddot{y}}{r^2}\right), \end{aligned}$$

здесь введены обозначения $(\frac{\partial}{\partial r})' = \frac{\partial}{\partial r}\left(\frac{\partial}{\partial r}\right)$, $(\frac{\partial}{\partial \theta})' = \frac{\partial}{\partial \theta}\left(\frac{\partial}{\partial \theta}\right)$.

Предположим, что точки края $r = R$ закреплены от смещения в направлении нормали к срединной поверхности и от поворотов, т. е. $w = w' = 0$. Стандартные варианты граничных условий требуют положить дополнительно равными нулю одну из двух величин в каждой из следующих пар: u или T_r , v или S , где u, v – проекции вектора перемещения на оси r и θ ; T_r, S – тангенциальные усилия. Жестко заделанный край моделируется условиями $u = v = w = w' = 0$, а случай $w = w' = T_r = S = 0$ соответствует свободному смещению точек края в радиальном и окружном направлениях.

Пусть по краю пластины имеется упругая связь (пружина), препятствующая ее свободному смещению в радиальном направлении, тогда перемещение u и усилие T_r на внешнем крае взаимосвязаны, т. е. $k_u u + T_r = 0$, где k_u – коэффициент упругости заделки. Таким образом, граничные условия запишутся в виде

$$w = w' = k_u u + T_r = S = 0. \quad (2)$$

Чтобы записать с помощью искомых функций w, F граничное условие (2), связывающее компоненту перемещения $u(r, \theta)$ с радиальным усилием T_r , воспользуемся представлением компонент деформации $\varepsilon_r, \varepsilon_\theta, \omega$ через компоненты вектора перемещения u, v, w , с одной стороны, и усилий T_r, T_θ, S – с другой:

$$\begin{aligned} \frac{\partial \varepsilon_\theta}{\partial r} - \frac{1}{r} \varepsilon_r - \frac{1}{r} \frac{\partial \omega}{\partial \theta} &= \frac{\partial}{\partial r} \left(\frac{T_\theta - \nu T_r}{E(r)h} \right) - \frac{1}{E(r)h} \frac{T_r - \nu T_\theta}{r} - \frac{2(1+\nu)}{E(r)h} \frac{1}{r} \frac{\partial S}{\partial \theta} = \\ &= -\frac{u}{r^2} - \frac{1}{r^2} \frac{\partial^2 u}{\partial \theta^2} - \frac{1}{2r} \left(\frac{\partial w}{\partial r} \right)^2 - \frac{1}{r} \frac{\partial w}{\partial r} \frac{\partial^2 w}{\partial \theta^2} - \frac{1}{r^3} \left(\frac{\partial w}{\partial \theta} \right)^2. \end{aligned} \quad (3)$$

Введем безразмерные переменные

$$\begin{aligned} r^* &= \frac{r}{R}, \quad w^* = \beta \frac{w}{h}, \quad p^* = \beta^3 \frac{pR^4}{E_{av} h^4}, \quad F^* = \beta^2 \frac{F}{E_{av} h^3}, \\ u^* &= \beta^2 \frac{R}{h^2} u, \quad k_u^* = \frac{R}{h E_{av}} k_u, \quad \beta^2 = 12(1 - \nu^2), \end{aligned} \quad (4)$$

где E_{av} – среднее значение модуля упругости:

$$E_{av} = \frac{1}{\pi R^2} \int_0^{2\pi} \int_0^R E(r) r dr d\theta.$$

Зависимость модуля упругости материала пластины от радиальной координаты может быть представлена в виде $E(r) = E_0 f(r)$, где $f(r)$ – достаточно гладкая и положительная на отрезке $[0, R]$ функция, E_0 – параметр, характеризующий величину модуля Юнга в центре пластины. Тогда система уравнений (1) примет вид (знак * у безразмерных величин (4) в дальнейшем опускаем)

$$\begin{aligned} g_1(r) \Delta \Delta w + g_1'(r) L_1^+(w) + g_1''(r) L_2^+(w) &= p + L(w, F), \\ g_2(r) \Delta \Delta F + g_2'(r) L_1^-(F) + g_2''(r) L_2^-(F) &= -\frac{L(w, w)}{2}, \end{aligned} \quad (5)$$

$$\text{здесь } g_1(r) = \frac{E_0 f(r)}{E_{av}}; \quad g_2(r) = \frac{1}{g_1(r)}.$$

Для сплошной пластины граничные условия (2) должны быть дополнены условиями ограниченности решений в центре

$$w' = F' = 0.$$

Симметричное решение. При значениях нагрузки, меньших критической величины p_{cr} , система (5), дополненная необходимыми граничными условиями, имеет только симметричное решение [4; 8; 12]. В этом случае, принимая $w(r, \theta) = w_s(r)$, $F(r, \theta) = F_s(r)$, симметричное решение задачи определяется из уравнений

$$\begin{aligned} g_1 \left(\omega_0'' + \frac{\omega_0'}{r} - \frac{\omega_0}{r^2} \right) + g_1' \left(\omega_0' + \frac{\nu}{r} \omega_0 \right) &= \frac{pr}{2} + \frac{\omega_0 \Phi_0}{r}, \\ g_2 \left(\Phi_0'' + \frac{\Phi_0'}{r} - \frac{\Phi_0}{r^2} \right) + g_2' \left(\Phi_0' + \frac{\nu}{r} \Phi_0 \right) &= -\frac{\omega_0^2}{2r} \end{aligned} \quad (6)$$

с учетом обозначений $\omega_0 = w_s'$, $\Phi_0 = F_s'$.

Граничные условия (2) на краю пластины $r = 1$ в силу соотношений (3) примут вид

$$\omega_0(1) = \Phi_0(1) = k_u g_2(1) (\Phi_0'(1) - \nu \Phi_0(1)) + \Phi_0(1) = 0. \quad (7)$$

В центре пластины необходимо положить

$$\omega_0(0) = \varphi_0(0) = 0. \quad (8)$$

Несимметричное решение. Следуя [4; 8], будем искать решение в виде

$$w(r, \theta) = w_s(r) + w_n(r) \cos n\theta, \quad F(r, \theta) = F_s(r) + F_n(r) \cos n\theta, \quad (9)$$

где функции $w_s(r)$, $F_s(r)$ определяют докритическое симметричное решение и могут быть найдены из решения системы (6) совместно с (7)–(8), а функции $w_{ns}(r, \theta) = w_n(r) \cos n\theta$, $F_{ns}(r, \theta) = F_n(r) \cos n\theta$ описывают поведение пластины сразу после ее перехода в неосесимметричное состояние, при этом $w_{ns}(r)$ и $F_{ns}(r)$ полагаются малыми. Число волн в окружном направлении, образовавшихся в результате бифуркации, обозначено n .

После подстановки (9) в систему (5) с учетом малости w_{ns} , F_{ns} получим линейную систему относительно $w_n(r)$, $F_n(r)$

$$\begin{aligned} g_1 \Delta_n \Delta_n w_n + g_1' L_{1n}^+(w_n) + g_1'' L_{2n}^+(w_n) = \\ = \omega_0' \left(\frac{F_n'}{r} - \frac{n^2}{r^2} F_n \right) + \varphi_0' \left(\frac{w_n'}{r} - \frac{n^2}{r^2} w_n \right) + \frac{w_n''}{r} \varphi_0 + \frac{F_n''}{r} \omega_0, \end{aligned} \quad (10)$$

$$g_2 \Delta_n \Delta_n F_n + g_2' L_{1n}^-(F_n) + g_2'' L_{2n}^-(F_n) = -\omega_0' \left(\frac{w_n'}{r} - \frac{n^2}{r^2} w_n \right) - \frac{w_n''}{r} \omega_0,$$

где

$$\begin{aligned} \Delta_n y = y'' + \frac{y'}{r} - \frac{n^2}{r^2} y; \\ L_{1n}^\pm(y) = 2y''' + \frac{2 \pm \nu}{r} y'' - \frac{2n^2 + 1}{r^2} y' + \frac{3n^2}{r^3} y; \quad L_{2n}^\pm(y) = y'' \pm \nu \left(\frac{y'}{r} - \frac{n^2}{r^2} y \right). \end{aligned}$$

Граничные условия (2) примут вид

$$w_n(1) = w_n'(1) = k_u u_n(1) + F_n'(1) - n^2 F_n(1) = F_n'(1) - F_n(1) = 0. \quad (11)$$

Здесь несимметричная составляющая компоненты перемещения $u_n(r)$ связана с функцией усилия $F_n(r)$ на краю пластины $r = 1$ соотношением

$$\begin{aligned} u_n = \frac{1}{n^2 - 1} \left(g_2 \left(F_n''' - ((2 + \nu)n^2 + 1 - \nu) F_n' + 3n^2 F_n \right) + \right. \\ \left. + g_2'(1) \left(F_n'' - \nu (F_n' - n^2 F_n) \right) \right), \end{aligned}$$

которое получено из записанной в безразмерном виде зависимости (3) с учетом $u(r, \theta) = u_s(r) + u_n(r) \cos n\theta$ и $w_n(1) = w_n'(1) = 0$.

В центре пластины, как и в симметричном случае,

$$w_n'(0) = F_n'(1) = 0.$$

Схема поиска несимметричного решения аналогична схемам, изложенным в работах [4; 8]. Сначала решается симметричная задача (6)–(8), а далее проверяется существование решения несимметричной задачи. Обозначим p_n нагрузку, при которой для заданного числа волн в окружном направлении n существуют отличные от нуля функции w_n , F_n , удовлетворяющие соотношениям (10), (11). Тогда под критической нагрузкой p_{cr} , при которой происходит бифуркация в неосесимметричное состояние, будем понимать наименьшее значение нагрузки p_n , когда появляются волны в окружном направлении, т. е. $p_{cr} = \min_n p_n$.

Результаты и их обсуждение

Предпосылки для перехода симметрично нагруженной пластины в неосесимметричное состояние создают сжимающие напряжения, которые появляются в окрестности края пластины при больших прогибах. На рис. 1 показано, как изменяется интенсивность безразмерных окружных усилий $T_\theta(r)$ при

различных значениях коэффициента жесткости пружины k_u . Величина $k_u = 0$ соответствует отсутствию ограничений на перемещение точек края пластины в радиальном направлении, т. е. условию $T_r = 0$. Абсолютно жесткой заделке края при $u = 0$ соответствует кривая, обозначенная как $k_u = \infty$.

Из рис. 1 видно, что с увеличением жесткости пружины k_u , ограничивающей свободное перемещение пластины в радиальном направлении, интенсивность сжимающих окружных напряжений уменьшается, а зона, в которой эти напряжения принимают отрицательные значения, сужается. Для величин параметра k_u , соответствующих условию жесткого защемления края пластины, окружные усилия принимают только положительные значения, и в этом случае бифуркация в неосесимметричное состояние невозможна [8; 10].

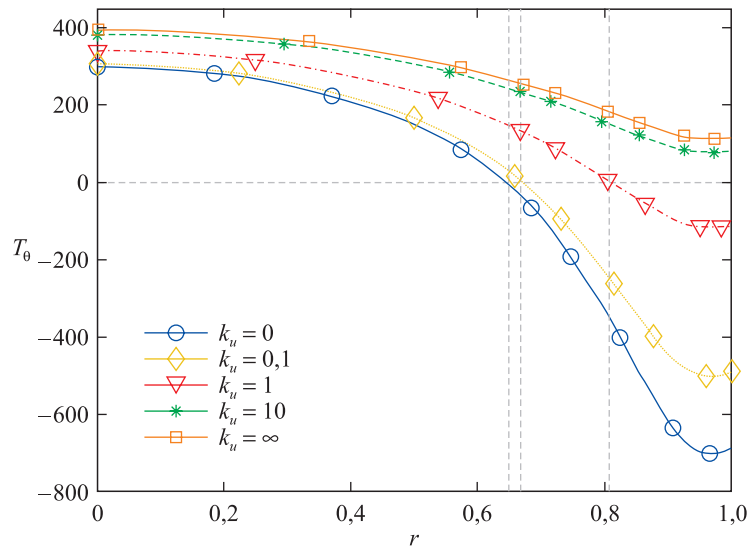


Рис. 1. Безразмерное окружное усилие $T_\theta(r)$ при различных значениях коэффициента жесткости пружины k_u . Для нагрузки принято $p = 30\,000$

Fig. 1. Dimensionless circumferential stress resultant $T_\theta(r)$ for different value of spring stiffness k_u . Load value is taken as $p = 30\,000$

Для однородной пластины с краем, который может свободно смещаться в радиальном направлении ($k_u = 0$), критическая нагрузка и соответствующее ей волновое число ($p_{cr} = 64\,453$, $n = 14$) найдены в [12]. Обозначим это значение критической нагрузки через p_{cr}^0 .

Как видно из рис. 2, с ростом жесткости пружины k_u пластина переходит в несимметричное состояние при более высоких величинах критической нагрузки и с образованием большего числа волн в окружном направлении (см. также таблицу). Так, для безразмерной жесткости $k_u = 0,1$, что при отношении $\frac{h}{R} = \frac{1}{100}$ соответствует жесткости пружины $10^{-3}E_{av}$, критическая нагрузка возрастает более чем в 2,5 раза, а число волн увеличивается до 17. Это согласуется с расчетами окружных усилий T_θ , представленными на рис. 1.

Результаты расчетов критической нагрузки для неоднородных пластин с модулем упругости $E(r) = E_0 e^{-qr}$ приведены в таблице и на рис. 3. Параметры E_0 , q закона изменения модуля выбирались так, чтобы его среднее значение E_{av} оставалось постоянным. При отсутствии сопротивления ($k_u = 0$) или достаточно слабом сопротивлении перемещению в окружном направлении края пластины ($k_u = 0,05$) потеря устойчивости осесимметричных форм равновесия происходит при более низких нагрузках, чем для однородной пластины (см. рис. 3 и таблицу).

С ростом жесткости пружины k_u , когда закрепление края приближается к жесткому защемлению, переход к несимметричной форме равновесия может происходить при нагрузке большей, чем для однородной пластины, если материал пластины достаточно сильно ослаблен к краю. Так, для $k_u = 0,15$ критическая нагрузка для неоднородной пластины сначала незначительно падает при $q = 0,05$, а затем увеличивается на 18 % с ростом параметра неоднородности пластины до $q = 2$. При этом для всех рассчитанных значений q и условий закрепления k_u потеря устойчивости осесимметричных форм равновесия неоднородной пластины происходит с образованием большего числа складок в окружном направлении, чем для однородной пластины (см. таблицу).

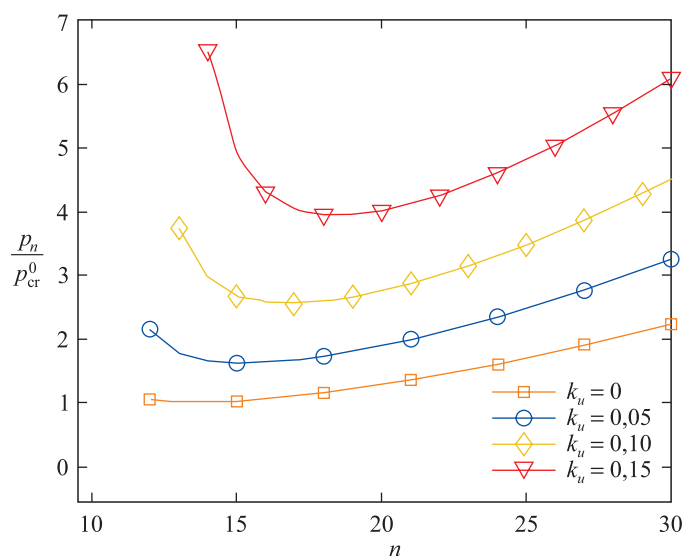


Рис. 2. Зависимость нагрузки $\frac{p_n}{p_{cr}^0}$ от волнового числа n в форме потери устойчивости для однородной пластины (p_{cr}^0 – критическая нагрузка, соответствующая однородной круглой пластине при $k_u = 0$)

Fig. 2. Dependence of the normalized critical load $\frac{p_n}{p_{cr}^0}$ on the mode number n for a uniform circular plate (p_{cr}^0 corresponds to the buckling load for a uniform circular plate with $k_u = 0$)

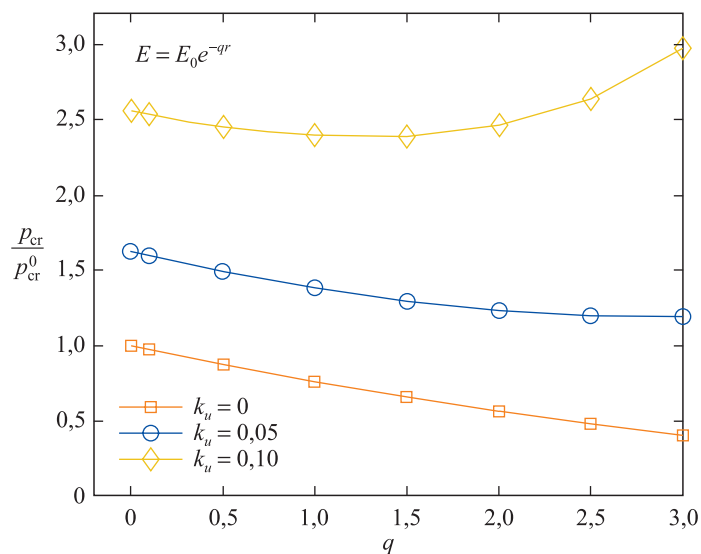


Рис. 3. Влияние коэффициента неоднородности q на критическую нагрузку $\frac{p_{cr}}{p_{cr}^0}$ (p_{cr}^0 – критическая нагрузка, соответствующая однородной круглой пластине)

Fig. 3. Change of the normalized buckling pressure $\frac{p_{cr}}{p_{cr}^0}$ when the degree of heterogeneity of the plate q changes (p_{cr}^0 – denotes the buckling pressure for a uniform circular plate)

Критическая нагрузка $\frac{P_{cr}}{P_{cr}^0}$ и волновое число n для неоднородной пластины
в зависимости от коэффициента жесткости заделки

The Buckling load $\frac{P_{cr}}{P_{cr}^0}$ and wave number n for different value of spring stiffness

Жесткость заделки k_u	Нагрузка				Волновое число			
	$q = 0$	$q = 0,5$	$q = 1$	$q = 2$	$q = 0$	$q = 0,5$	$q = 1$	$q = 2$
0	1	0,87	0,76	0,56	14	14	14	14
0,05	1,62	1,49	1,38	1,23	14	15	16	16
0,10	2,56	2,45	2,39	2,47	17	17	17	19
0,15	3,96	3,92	4,01	4,69	18	19	19	21

Заключение

В работе представлены результаты численного исследования потери устойчивости осесимметричных форм равновесия изотропных пластин с переменным модулем упругости при различных условиях закрепления внешнего края. Показано, что с увеличением жесткости пружины, ограничивающей перемещение края пластины в радиальном направлении, бифуркация в несимметричное состояние может происходить при значительно больших нагрузках и с образованием большего числа волн в окружном направлении. Уменьшение жесткости оболочки к краю приводит к существенному снижению величины критической нагрузки, если радиальные перемещения края пластины ничем не ограничены.

Библиографические ссылки

1. Adachi J. *Stresses and buckling in thin domes under internal pressure*. Watertown: U.S. Army Materials and Mechanics Research Center; 1968.
2. Bushnell D. Buckling of shells-pitfall for designers. *AIAA Journal*. 2015;19(9):1183–1226. DOI: 10.2514/3.60058.
3. Панов ДЮ, Феодосьев ВИ. О равновесии и потере устойчивости пологих оболочек при больших прогибах. *Прикладная математика и механика*. 1948;12:389–406.
4. Huang NC. Unsymmetrical buckling of shallow spherical shells. *Journal of Applied Mechanics*. 1964;31(3):447–457. DOI: 10.1115/1.3629662.
5. Feodos'ev VI. On a method of solution of the nonlinear problems of stability of deformable systems. *Journal of Applied Mathematics and Mechanics*. 1963;27(2):392–404. DOI: 10.1016/0021-8928(63)90008-X.
6. Морозов НФ. К вопросу о существовании несимметричного решения в задаче о больших прогибах круглой пластинки, нагруженной симметричной нагрузкой. *Известия высших учебных заведений. Математика*. 1961;2:126–129.
7. Piechocki W. On the nonlinear theory of thin elastic spherical shells: nonlinear partial differential equations solutions in theory of thin elastic spherical shells subjected to temperature fields and external loading. *Archives of Mechanics*. 1969;21(1):81–102.
8. Cheo LS, Reiss EL. Unsymmetric wrinkling of circular plates. *The Quarterly Journal of Mechanics and Applied Mathematics*. 1973;31(1):75–91. DOI: 10.1090/qam/99710.
9. Coman CD. Asymmetric bifurcations in a pressurised circular thin plate under initial tension. *Mechanics Research Communications*. 2013;47:11–17. DOI: 10.1016/j.mechrescom.2012.09.005.
10. Coman CD, Bassom AP. Asymptotic limits and wrinkling patterns in a pressurised shallow spherical cap. *International Journal of Non-Linear Mechanics*. 2016;81:8–18. DOI: 10.1016/j.ijnonlinmec.2015.12.004.
11. Гольдштейн РВ, Попов АЛ, Козинцев ВМ, Челюбеев ДА. Неосесимметричная потеря устойчивости при осесимметричном нагреве круглой пластины. *Вестник Пермского национального исследовательского политехнического университета. Механика*. 2016;2:45–53. DOI: 10.15593/perm.mech/2016.2.04.
12. Bauer SM, Voronkova EB. Models of shells and plates in the problems of ophthalmology. *Vestnik St. Petersburg University. Mathematics*. 2014;47(3):123–139. DOI: 10.3103/S1063454114030029.
13. Bauer SM, Voronkova EB. Unsymmetrical wrinkling of nonuniform annular plates and spherical caps under internal pressure. In: Altenbach H, Chróścielewski J, Eremeyev V, Wiśniewski K, editors. *Recent developments in the theory of shells. Advanced structured materials. Volume 110*. Cham: Springer; 2019. p. 79–89. DOI: 10.1007/978-3-030-17747-8_6.

References

1. Adachi J. *Stresses and buckling in thin domes under internal pressure*. Watertown: U.S. Army Materials and Mechanics Research Center; 1968.
2. Bushnell D. Buckling of shells-pitfall for designers. *AIAA Journal*. 2015;19(9):1183–1226. DOI: 10.2514/3.60058.
3. Panov DYU, Feodos'ev VI. [On the equilibrium and loss of stability of shallow shells in the case of large displacement]. *Prikladnaya matematika i mekhanika*. 1948;12:389–406. Russian.

4. Huang NC. Unsymmetrical buckling of shallow spherical shells. *Journal of Applied Mechanics*. 1964;31(3):447–457. DOI: 10.1115/1.3629662.
5. Feodos'ev VI. On a method of solution of the nonlinear problems of stability of deformable systems. *Journal of Applied Mathematics and Mechanics*. 1963;27(2):392–404. DOI: 10.1016/0021-8928(63)90008-X.
6. Morozov NF. [On the existence of a non-symmetric solution in the problem of large deflections of a circular plate with a symmetric load]. *Izvestiya vysshikh uchebnykh zavedenii. Matematika*. 1961;2:126–129. Russian.
7. Piechocki W. On the nonlinear theory of thin elastic spherical shells: nonlinear partial differential equations solutions in theory of thin elastic spherical shells subjected to temperature fields and external loading. *Archives of Mechanics*. 1969;21(1):81–102.
8. Cheo LS, Reiss EL. Unsymmetric wrinkling of circular plates. *The Quarterly Journal of Mechanics and Applied Mathematics*. 1973;31(1):75–91. DOI: 10.1090/qam/99710.
9. Coman CD. Asymmetric bifurcations in a pressurised circular thin plate under initial tension. *Mechanics Research Communications*. 2013;47:11–17. DOI: 10.1016/j.mechrescom.2012.09.005.
10. Coman CD, Bassom AP. Asymptotic limits and wrinkling patterns in a pressurised shallow spherical cap. *International Journal of Non-Linear Mechanics*. 2016;81:8–18. DOI: 10.1016/j.ijnonlinmec.2015.12.004.
11. Goldstein RV, Popov AL, Kozintsev VM, Chelyubeev DA. Non-axisymmetric edge buckling of circular plates when heated. *PNRPU Mechanics Bulletin*. 2016;2:45–53. DOI: 10.15593/perm.mech/2016.2.04. Russian.
12. Bauer SM, Voronkova EB. Models of shells and plates in the problems of ophthalmology. *Vestnik St. Petersburg University. Mathematics*. 2014;47(3):123–139. DOI: 10.3103/S1063454114030029.
13. Bauer SM, Voronkova EB. Unsymmetrical wrinkling of nonuniform annular plates and spherical caps under internal pressure. In: Altenbach H, Chróścielewski J, Eremeyev V, Wiśniewski K, editors. *Recent developments in the theory of shells. Advanced structured materials. Volume 110*. Cham: Springer; 2019. p. 79–89. DOI: 10.1007/978-3-030-17747-8_6.

Статья поступила в редколлегию 04.01.2020.
Received by editorial board 04.01.2020.

**РЕШЕНИЕ НЕОСЕССИМЕТРИЧНОЙ СТАЦИОНАРНОЙ
ЗАДАЧИ ТЕПЛОПРОВОДНОСТИ ДЛЯ ПОЛЯРНО-ОРТОТРОПНОЙ
КОЛЬЦЕВОЙ ПЛАСТИНЫ ПЕРЕМЕННОЙ ТОЛЩИНЫ
С УЧЕТОМ ТЕПЛООБМЕНА С ВНЕШНЕЙ СРЕДОЙ****В. В. КОРОЛЕВИЧ¹⁾**¹⁾Международный центр современного образования,
ул. Штепанска, 61, 110 00, г. Прага 1, Чехия

Приводится решение неосесимметричной стационарной задачи теплопроводности для профилированных полярно-ортотропных кольцевых пластин с учетом теплообмена их с внешней средой через основания. Предполагается, что теплофизические характеристики материала пластины не зависят от температуры. На внутреннем контуре пластины поддерживается постоянная температура T_1^* , а на внешнем контуре приложено N равноотстоящих точечных источников тепла с одинаковой температурой T_2^* каждый. Температура пластины больше температуры окружающей среды T_0 ($T_0 < T_1^* < T_2^*$). Полагается, что в тонкой кольцевой пластине температура не меняется по толщине. Внутренние источники тепла в ней отсутствуют. Распределение температур в таких пластинах неосесимметрично. Даны аналитические решения стационарной задачи теплопроводности для кольцевых анизотропных пластин постоянной толщины, обратноконической и конической кольцевых пластин. Для получения решения в общем случае записывается интегральное уравнение Вольтерры 2-го рода, соответствующее заданному дифференциальному уравнению стационарной теплопроводности для профилированных анизотропных кольцевых пластин. Представляются в явном виде ядра интегрального уравнения для анизотропных кольцевых пластин степенного и экспоненциального профилей. Решение интегрального уравнения записывается с помощью резольвенты. Из-за наличия иррациональных функций в ядрах интегрального уравнения необходимо применять численные методы при нахождении итерированных ядер либо численно решать интегральное уравнение Вольтерры 2-го рода. Приводится формула расчета температур в анизотропных кольцевых пластинах произвольного профиля.

Ключевые слова: полярно-ортотропная кольцевая пластина; температура; стационарное уравнение теплопроводности; дифференциальное уравнение; интегральное уравнение Вольтерры 2-го рода; пластина постоянной толщины; обратноконическая пластина; коническая пластина; пластина степенного профиля; пластина экспоненциального профиля.

Образец цитирования:

Королевич ВВ. Решение неосесимметричной стационарной задачи теплопроводности для полярно-ортотропной кольцевой пластины переменной толщины с учетом теплообмена с внешней средой. *Журнал Белорусского государственного университета. Математика. Информатика.* 2020;1:47–58. <https://doi.org/10.33581/2520-6508-2020-1-47-58>

For citation:

Karalevich UV. Solution of nonaxisymmetric stationary problem of heat conductivity for polar-orthotropic ring plate of variable thickness with account of heat transfer with external environment. *Journal of the Belarusian State University. Mathematics and Informatics.* 2020;1:47–58. Russian. <https://doi.org/10.33581/2520-6508-2020-1-47-58>

Автор:

Владимир Васильевич Королевич – преподаватель.

Author:

Uladzimir V. Karalevich, lecturer.
v.korolevich@mail.ru

SOLUTION OF NONAXISYMMETRIC STATIONARY PROBLEM OF HEAT CONDUCTIVITY FOR POLAR-ORTHOTROPIC RING PLATE OF VARIABLE THICKNESS WITH ACCOUNT OF HEAT TRANSFER WITH EXTERNAL ENVIRONMENT

U. V. KARALEVICH^a

^aInternational Center of Modern Education, 61 Štěpánská Street, Prague 1, PSČ 110 00, Czech

The solution of the nonaxisymmetric stationary problem of the heat conductivity for profiled polar-orthotropic annular plates considering the heat exchange with external environment through the bases is presented. Thermophysical characteristics of the material of the plate are assumed to be temperature-independent. A constant temperature T_1^* is maintained on the inner contour of the ring plate and on the outer contour N equidistant point sources of heat with the same temperature T_2^* each are applied. Plate temperature is higher than ambient temperature T_0 ($T_0 < T_1^* < T_2^*$). It is assumed that the temperature does not vary in thickness of a thin ring plate. The temperature values on the contours of the annular plate are given. There are no internal heat sources in the plate. The temperature distribution in such plates will be nonaxisymmetric. Analytical solutions of the stationary heat conductivity problem for the following anisotropic annular plates are presented: the plate of constant thickness, the back conical and the conical plate. The Volterra integral equation of the second kind corresponding to the given differential equation of the stationary heat conductivity for profiled anisotropic annular plates is written to obtain the solution in the general case. The kernels of the integral equation for anisotropic annular plates of power and exponential profiles are given explicitly. The solution of the integral equation is written by using the resolvent. It is indicated that due to the presence of irrational functions in the kernels of the integral equation it is necessary to apply numerical methods in the calculation of iterated kernels or numerically solve the Volterra integral equation of the second kind. A formula for the calculation of temperatures in anisotropic annular plates of an arbitrary profile is given.

Keywords: polar-orthotropic annular plate; temperature; stationary equation of heat conductivity; differential equation; Volterra integral equation of the second kind; plate of a constant thickness; back conical plate; conical plate; plate of a power profile; plate of an exponential profile.

Введение

В современном энергетическом оборудовании, машиностроительных и авиационных конструкциях, аппаратах пищевой и химической промышленности в качестве составных элементов широко применяются кольцевые пластины из композитных материалов. В процессе работы механизмов эти пластины могут находиться в неоднородных тепловых полях, что приводит к появлению в них дополнительных температурных напряжений, которые необходимо учитывать при проектировании и эксплуатации указанных конструкций. Для этого надо знать закон распределения температуры в профилированной анизотропной кольцевой пластине. Данная работа посвящена решению такой задачи для указанных анизотропных кольцевых пластин.

Постановка задачи

Рассмотрим анизотропную кольцевую пластину, толщина $h(r)$ которой изменяется вдоль радиуса r по заданному закону. Пластина изготовлена из композитного материала, обладающего цилиндрической анизотропией, причем ось анизотропии совпадает с геометрической осью пластины, и в ее каждой точке имеются три взаимно ортогональные плоскости упругой симметрии.

Пусть на внутреннем контуре ($r = r_0$) пластины поддерживается постоянная температура T_1^* , а на внешнем контуре ($r = R$) приложено N равноотстоящих точечных источников тепла с одинаковой температурой T_2^* каждый. Естественно, идеальных точечных источников тепла в природе нет, и все они имеют какую-то протяженность.

Частично эта задача рассматривалась нами в работе [1], и было получено распределение температуры $T^{\text{внеш}}$ на внешнем контуре в случае, когда N источников тепла приложены на одинаковых дугах длиной l и с соответствующим центральным углом φ ($l = \varphi R$) каждая:

$$T^{\text{внеш}}(R, \theta, \varphi) = NT_2^* \left(1 + 2 \sum_{n=1}^{\infty} \frac{\sin n\varphi}{n\varphi} \cos Nn\theta \right).$$

Влияние протяженных источников тепла на внешней границе на распределение температуры в анизотропной кольцевой пластине переменной толщины – тема следующих наших исследований.

Температура пластины больше температуры окружающей среды T_0 ($T_0 < T_1^* < T_2^*$). Внутренних источников тепла в ней не имеется. Тепловое поле в такой полярно-ортотропной кольцевой пластине будет неосесимметричным.

В настоящей работе решается неосесимметричная стационарная задача теплопроводности для полярно-ортотропной кольцевой пластины переменной толщины с учетом теплообмена через оба ее основания с внешней средой. Для тонкой кольцевой пластины теплообмен через боковую цилиндрическую поверхность пренебрежимо мал и его можно не учитывать в расчетах. Предполагается, что температура в такой пластине не меняется по толщине. Таким образом, пространственная задача теплопроводности сводится к плоской задаче теплопроводности, содержащей два коэффициента теплопроводности – радиальный λ_r и тангенциальный λ_θ , а также коэффициент теплоотдачи H [2; 3]. Эти коэффициенты полагаются постоянными и не зависящими от температуры.

Решение задачи

Введем цилиндрическую систему координат r, θ, z , поместив начало в точке пересечения оси анизотропии со срединной плоскостью пластины. Ось z направим вверх.

Уравнение стационарной теплопроводности для полярно-ортотропной кольцевой пластины переменной толщины $h(r)$ с учетом теплообмена с внешней средой через оба основания пластины запишется в виде [2; 3]

$$\frac{1}{r} \frac{\partial}{\partial r} \left(r h(r) \lambda_r \frac{\partial T}{\partial r} \right) + \frac{1}{r^2} \frac{\partial}{\partial \theta} \left(h(r) \lambda_\theta \frac{\partial T}{\partial \theta} \right) - 2H(T(r, \theta) - T_0) \left(1 + \frac{1}{4} \left(\frac{dh}{dr} \right)^2 \right)^{\frac{1}{2}} = 0, \quad (1)$$

где $T(r, \theta)$ – функция температуры в анизотропной кольцевой пластине.

Рассмотрим новую функцию $\Theta(r, \theta)$, которая тоже имеет смысл функции температуры:

$$\Theta(r, \theta) = T(r, \theta) - T_0. \quad (2)$$

В силу выражения (2) уравнение (1) примет вид

$$\frac{\partial^2 \Theta}{\partial r^2} + \left(\frac{h'(r)}{h(r)} + \frac{1}{r} \right) \frac{\partial \Theta}{\partial r} + \frac{\lambda_\theta}{\lambda_r} \frac{1}{r^2} \frac{\partial^2 \Theta}{\partial \theta^2} - \frac{2H}{\lambda_r h(r)} \left(1 + \frac{1}{4} \left(\frac{dh}{dr} \right)^2 \right)^{\frac{1}{2}} \Theta(r, \theta) = 0. \quad (3)$$

Разложим функцию $\Theta(r, \theta)$ в тригонометрический ряд Фурье:

$$\Theta(r, \theta) = \Theta_0(r) + \sum_{n=1}^{\infty} \Theta_n^{(1)}(r) \cos Nn\theta + \sum_{n=1}^{\infty} \Theta_n^{(2)}(r) \sin Nn\theta. \quad (4)$$

Здесь первый член $\Theta_0(r)$ разложения (4) учитывает осесимметричную составляющую функции $\Theta(r, \theta)$; слагаемые, содержащие $\cos Nn\theta$, соответствуют симметричным составляющим относительно плоскости $\theta = 0$, а слагаемые, содержащие $\sin Nn\theta$, – антисимметричным.

Подстановка разложения (4) в уравнение (3) приводит к бесконечной системе однородных обыкновенных дифференциальных уравнений 2-го порядка с переменными коэффициентами:

$$\left\{ \begin{aligned} (n=0) \quad & \frac{d^2 \Theta_0}{dr^2} + \left(\frac{h'(r)}{h(r)} + \frac{1}{r} \right) \frac{d\Theta_0}{dr} - \frac{2H}{\lambda_r h(r)} \left(1 + \frac{1}{4} \left(\frac{dh}{dr} \right)^2 \right)^{\frac{1}{2}} \Theta_0(r) = 0, \end{aligned} \right. \quad (5)$$

$$\left\{ \begin{aligned} (n \geq 1, j = \overline{1, 2}) \quad & \frac{d^2 \Theta_n^{(j)}}{dr^2} + \left(\frac{h'(r)}{h(r)} + \frac{1}{r} \right) \frac{d\Theta_n^{(j)}}{dr} - \left(\frac{\lambda_\theta (Nn)^2}{\lambda_r r^2} + \frac{2H}{\lambda_r h(r)} \left(1 + \frac{1}{4} \left(\frac{dh}{dr} \right)^2 \right)^{\frac{1}{2}} \right) \Theta_n^{(j)}(r) = 0. \end{aligned} \right. \quad (6)$$

Дифференциальное уравнение (5), описывающее осесимметричное распределение температуры в профилированных полярно-ортотропных кольцевых пластинах с учетом теплообмена с внешней средой, подробно исследовалось нами в работе [4]. Получим сейчас точные решения дифференциального уравнения (6) для частных случаев профилированных анизотропных кольцевых пластин.

Кольцевая пластина постоянной толщины h_0 . Дифференциальное уравнение (6) в этом случае примет вид

$$r^2 \frac{d^2 \Theta_n^{(j)}}{dr^2} + r \frac{d \Theta_n^{(j)}}{dr} - \left(\frac{2H}{\lambda_r h_0} r^2 + \frac{\lambda_\theta}{\lambda_r} (Nn)^2 \right) \Theta_n^{(j)}(r) = 0. \quad (7)$$

Введем новую переменную $x = \sqrt{\frac{2H}{\lambda_r h_0}} r$ и параметр $\nu(n) = N \sqrt{\frac{\lambda_\theta}{\lambda_r}} n$. Ниже аргумент n у параметра будем опускать. Уравнение (7) сводится к модифицированному уравнению Бесселя

$$x^2 \frac{d^2 \Theta_n^{(j)}}{dx^2} + x \frac{d \Theta_n^{(j)}}{dx} - (x^2 + \nu^2) \Theta_n^{(j)}(x) = 0.$$

Его решение выражается через модифицированную функцию Бесселя 1-го рода ν -го порядка $I_\nu(x)$ и модифицированную функцию Бесселя 2-го рода ν -го порядка $K_\nu(x)$ (функцию Макдональда) [5]:

$$\Theta_n^{(j)}(x) = C_1^{(j)} I_\nu(x) + C_2^{(j)} K_\nu(x),$$

где $C_1^{(j)}, C_2^{(j)}$ – произвольные постоянные, определяемые из граничных условий.

Возвращаясь к переменной r , запишем общее решение уравнения (7) в виде

$$\Theta_n^{(j)}(r) = C_1^{(j)} I_\nu \left(\sqrt{\frac{2H}{\lambda_r h_0}} r \right) + C_2^{(j)} K_\nu \left(\sqrt{\frac{2H}{\lambda_r h_0}} r \right). \quad (8)$$

Пусть на внешнем контуре анизотропной кольцевой пластины приложены N точечных источников тепла с температурой T_2^* каждый. Как показано в [1], распределение температуры $T^{\text{внеш}}(R, \theta)$ на этом контуре задается тригонометрическим рядом Фурье:

$$T^{\text{внеш}}(R, \theta) = NT_2^* \left(1 + 2 \sum_{n=1}^{\infty} \cos Nn\theta \right).$$

Число N источников тепла с температурой T_2^* не может быть произвольным, а ограничивается температурой плавления $T_{\text{плавл}}$ материала пластины. Действительно, $NT_2^* \leq T_{\text{плавл}}$, отсюда $N \leq \frac{T_{\text{плавл}}}{T_2^*}$. Таким образом, источников тепла на внешнем контуре может быть от 2 до $N_{\text{max}} = \left\lfloor \frac{T_{\text{плавл}}}{T_2^*} \right\rfloor$, где квадратные скобки означают целую часть дробного выражения.

Получим теперь граничные условия для функции температуры $\Theta(r, \theta)$. Из формулы (2) следует

$$T(r, \theta) = \Theta(r, \theta) + T_0.$$

Подставив в последнее равенство разложение функции $\Theta(r, \theta)$ в тригонометрический ряд Фурье (см. (4)), получим

$$T(r, \theta) = \Theta_0(r) + T_0 + \sum_{n=1}^{\infty} \Theta_n^{(1)}(r) \cos Nn\theta + \sum_{n=1}^{\infty} \Theta_n^{(2)}(r) \sin Nn\theta.$$

Для функции $T(r, \theta)$ на границе пластины должны выполняться условия

$$\left\{ \begin{aligned} T(r_0, \theta) &= \Theta_0(r_0) + T_0 + \sum_{n=1}^{\infty} \Theta_n^{(1)}(r_0) \cos Nn\theta + \sum_{n=1}^{\infty} \Theta_n^{(2)}(r_0) \sin Nn\theta = T^{\text{внутр}}(r_0, \theta) = \\ &= T_1^* + \sum_{n=1}^{\infty} 0 \cdot \cos Nn\theta + \sum_{n=1}^{\infty} 0 \cdot \sin Nn\theta, \\ T(R, \theta) &= \Theta_0(R) + T_0 + \sum_{n=1}^{\infty} \Theta_n^{(1)}(R) \cos Nn\theta + \sum_{n=1}^{\infty} \Theta_n^{(2)}(R) \sin Nn\theta = T^{\text{внеш}}(R, \theta) = \\ &= NT_2^* + \sum_{n=1}^{\infty} 2NT_2^* \cos Nn\theta + \sum_{n=1}^{\infty} 0 \cdot \sin Nn\theta. \end{aligned} \right.$$

В результате сравнения коэффициентов тригонометрических рядов при одинаковых гармониках левых и правых частей приведенных выражений найдем граничные условия

$$(n=0) \quad \begin{cases} \Theta_0(r_0) = T_1^* - T_0, \\ \Theta_0(R) = NT_2^* - T_0, \end{cases} \quad (9)$$

$$(n \geq 1) \quad \begin{cases} \Theta_n^{(1)}(r_0) = 0, \\ \Theta_n^{(1)}(R) = 2NT_2^*, \end{cases} \quad (10)$$

$$(n \geq 1) \quad \begin{cases} \Theta_n^{(2)}(r_0) = 0, \\ \Theta_n^{(2)}(R) = 0. \end{cases} \quad (11)$$

При нулевых граничных условиях (11) однородное дифференциальное уравнение (7) имеет тривиальное решение [6], следовательно, функция $\Theta_n^{(2)}(r)$ равна нулю, т. е. антисимметричная составляющая в разложении (4) для функции $\Theta(r, \theta)$ отсутствует.

Удовлетворим решение (8) граничным условиям (9), (10):

$$(n=0) \quad \begin{cases} C_1^{(0)} I_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} r_0 \right) + C_2^{(0)} K_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} r_0 \right) = T_1^* - T_0, \\ C_1^{(0)} I_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} R \right) + C_2^{(0)} K_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} R \right) = NT_2^* - T_0, \end{cases} \quad (12)$$

$$(n \geq 1) \quad \begin{cases} C_1^{(1)} I_v \left(\sqrt{\frac{2H}{\lambda_r h_0}} r_0 \right) + C_2^{(1)} K_v \left(\sqrt{\frac{2H}{\lambda_r h_0}} r_0 \right) = 0, \\ C_1^{(1)} I_v \left(\sqrt{\frac{2H}{\lambda_r h_0}} R \right) + C_2^{(1)} K_v \left(\sqrt{\frac{2H}{\lambda_r h_0}} R \right) = 2NT_2^*. \end{cases} \quad (13)$$

Решая системы алгебраических уравнений (12), (13) методом Крамера, найдем

$$\begin{cases} C_1^{(0)} = \frac{1}{\Delta_0} \left(T_1^* K_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} R \right) - NT_2^* K_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} r_0 \right) + T_0 \left(K_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} r_0 \right) - K_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} R \right) \right) \right), \\ C_2^{(0)} = -\frac{1}{\Delta_0} \left(T_1^* I_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} R \right) - NT_2^* I_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} r_0 \right) + T_0 \left(I_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} r_0 \right) - I_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} R \right) \right) \right), \end{cases} \quad (14)$$

$$\begin{cases} C_1^{(1)} = -NT_2^* \frac{2}{\Delta_v} K_v \left(\sqrt{\frac{2H}{\lambda_r h_0}} r_0 \right), \\ C_2^{(1)} = NT_2^* \frac{2}{\Delta_v} I_v \left(\sqrt{\frac{2H}{\lambda_r h_0}} r_0 \right), \end{cases} \quad (15)$$

где Δ_0, Δ_v – определители 2-го порядка:

$$\begin{aligned} \Delta_0 &= I_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} r_0 \right) K_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} R \right) - I_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} R \right) K_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} r_0 \right), \\ \Delta_v &= I_v \left(\sqrt{\frac{2H}{\lambda_r h_0}} r_0 \right) K_v \left(\sqrt{\frac{2H}{\lambda_r h_0}} R \right) - I_v \left(\sqrt{\frac{2H}{\lambda_r h_0}} R \right) K_v \left(\sqrt{\frac{2H}{\lambda_r h_0}} r_0 \right). \end{aligned}$$

Подставляя в формулу (2) найденные решения (8) с учетом выражений (14), (15) для постоянных $C_1^{(j)}, C_2^{(j)}$ ($j = \overline{1, 2}$), получим распределение температуры $T(r, \theta)$ в полярно-ортотропной кольцевой пластине постоянной толщины h_0 при учете теплообмена с внешней средой:

$$\begin{aligned} T(r, \theta) = & \frac{T_1^*}{\Delta_0} \left(I_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} r \right) K_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} R \right) - I_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} R \right) K_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} r \right) \right) + \\ & + \frac{NT_2^*}{\Delta_0} \left(I_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} r_0 \right) K_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} r \right) - I_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} r \right) K_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} r_0 \right) \right) + \\ & + T_0 \left(1 + \frac{1}{\Delta_0} \left(I_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} R \right) - I_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} r_0 \right) \right) K_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} r \right) - \right. \\ & \left. - \frac{1}{\Delta_0} \left(K_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} R \right) - K_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} r_0 \right) \right) I_0 \left(\sqrt{\frac{2H}{\lambda_r h_0}} r \right) \right) - \\ & - NT_2^* \sum_{n=1}^{\infty} \frac{2}{\Delta_v} \left[I_v \left(\sqrt{\frac{2H}{\lambda_r h_0}} r \right) K_v \left(\sqrt{\frac{2H}{\lambda_r h_0}} r_0 \right) - I_v \left(\sqrt{\frac{2H}{\lambda_r h_0}} r_0 \right) K_v \left(\sqrt{\frac{2H}{\lambda_r h_0}} r \right) \right] \cos Nn\theta. \end{aligned}$$

Обратноконическая кольцевая пластина. Толщина $h(r)$ этой пластины изменяется вдоль радиуса r по закону $h(r) = h_0 \left(\frac{r}{r_0} \right)$, где h_0 – толщина пластины на внутреннем контуре ($r = r_0$). Дифференцируя функцию $h(r)$ и подставляя в уравнение (6), получим

$$r^2 \frac{d^2 \Theta_n^{(1)}}{dr^2} + 2r \frac{d\Theta_n^{(1)}}{dr} - \left(\frac{H \sqrt{h_0^2 + 4r_0^2}}{\lambda_r h_0} r + \frac{\lambda_\theta}{\lambda_r} (Nn)^2 \right) \Theta_n^{(1)}(r) = 0. \quad (16)$$

Обозначим $\frac{H \sqrt{h_0^2 + 4r_0^2}}{\lambda_r h_0} = b$, $N \sqrt{\frac{\lambda_\theta}{\lambda_r}} n = v(n)$. Тогда (16) запишется в виде

$$r^2 \frac{d^2 \Theta_n^{(1)}}{dr^2} + 2r \frac{d\Theta_n^{(1)}}{dr} - (br + v^2) \Theta_n^{(1)}(r) = 0. \quad (17)$$

Введем новую функцию $Z_n^{(1)}(2\sqrt{b}\sqrt{r})$, которая связана с $\Theta_n^{(1)}(r)$ зависимостью

$$\Theta_n^{(1)}(r) = \frac{1}{\sqrt{r}} Z_n^{(1)}(2\sqrt{b}\sqrt{r}). \quad (18)$$

Подстановка выражения (18) в уравнение (17) приводит к модифицированному уравнению Бесселя для функции $Z_n^{(1)}(t)$:

$$t^2 \frac{d^2 Z_n^{(1)}}{dt^2} + t \frac{dZ_n^{(1)}}{dt} - (t^2 + \mu^2) Z_n^{(1)}(t) = 0, \quad (19)$$

где $t = 2\sqrt{b}\sqrt{r}$; $\mu = \mu(n) = \sqrt{1 + 4N^2 \left(\frac{\lambda_\theta}{\lambda_r} \right) n^2}$. Ниже аргумент n у параметра $\mu(n)$ будем опускать.

Решение уравнения (19) выражается через модифицированную функцию Бесселя 1-го рода μ -го порядка $I_\mu(t)$ и модифицированную функцию Бесселя 2-го рода μ -го порядка $K_\mu(t)$ (функцию Макдональда) [5]:

$$Z_n^{(1)}(t) = \tilde{C}_1^{(1)} I_\mu(t) + \tilde{C}_2^{(1)} K_\mu(t),$$

где $\tilde{C}_1^{(1)}, \tilde{C}_2^{(1)}$ – произвольные постоянные.

Возвращаясь к замене (18), запишем решение уравнения (16):

$$\Theta_n^{(1)}(r) = \frac{1}{\sqrt{r}} \left(\tilde{C}_1^{(1)} I_\mu(2\sqrt{b}\sqrt{r}) + \tilde{C}_2^{(1)} K_\mu(2\sqrt{b}\sqrt{r}) \right). \quad (20)$$

Постоянные $\tilde{C}_1^{(1)}, \tilde{C}_2^{(1)}$ определим из граничных условий (9), (10). Подставляя решения (20) в (9), (10), получим системы алгебраических уравнений относительно неизвестных $\tilde{C}_1^{(0)}, \tilde{C}_2^{(0)}$ и $\tilde{C}_1^{(1)}, \tilde{C}_2^{(1)}$:

$$(n=0) \quad \begin{cases} \frac{1}{\sqrt{r_0}} \left(\tilde{C}_1^{(0)} I_1(2\sqrt{b}\sqrt{r_0}) + \tilde{C}_2^{(0)} K_1(2\sqrt{b}\sqrt{r_0}) \right) = T_1^* - T_0, \\ \frac{1}{\sqrt{R}} \left(\tilde{C}_1^{(0)} I_1(2\sqrt{b}\sqrt{R}) + \tilde{C}_2^{(0)} K_1(2\sqrt{b}\sqrt{R}) \right) = NT_2^* - T_0, \end{cases} \quad (21)$$

$$(n \geq 1) \quad \begin{cases} \frac{1}{\sqrt{r_0}} \left(\tilde{C}_1^{(1)} I_\mu(2\sqrt{b}\sqrt{r_0}) + \tilde{C}_2^{(1)} K_\mu(2\sqrt{b}\sqrt{r_0}) \right) = 0, \\ \frac{1}{\sqrt{R}} \left(\tilde{C}_1^{(1)} I_\mu(2\sqrt{b}\sqrt{R}) + \tilde{C}_2^{(1)} K_\mu(2\sqrt{b}\sqrt{R}) \right) = 2NT_2^*. \end{cases} \quad (22)$$

Методом Крамера найдем решение системы алгебраических уравнений (21), (22)

$$\begin{cases} \tilde{C}_1^{(0)} = \frac{\sqrt{r_0}}{\Delta_2} K_1(2\sqrt{b}\sqrt{R})(T_1^* - T_0) - \frac{\sqrt{R}}{\Delta_2} K_1(2\sqrt{b}\sqrt{r_0})(NT_2^* - T_0), \\ \tilde{C}_2^{(0)} = -\frac{\sqrt{r_0}}{\Delta_2} I_1(2\sqrt{b}\sqrt{R})(T_1^* - T_0) + \frac{\sqrt{R}}{\Delta_2} I_1(2\sqrt{b}\sqrt{r_0})(NT_2^* - T_0), \end{cases} \quad (23)$$

$$\begin{cases} \tilde{C}_1^{(1)} = -NT_2^* \frac{2\sqrt{R}}{\Delta_\mu} K_\mu(2\sqrt{b}\sqrt{r_0}), \\ \tilde{C}_2^{(1)} = NT_2^* \frac{2\sqrt{R}}{\Delta_\mu} I_\mu(2\sqrt{b}\sqrt{r_0}), \end{cases} \quad (24)$$

где Δ_2, Δ_μ – определители 2-го порядка:

$$\Delta_2 = I_1(2\sqrt{b}\sqrt{r_0}) K_1(2\sqrt{b}\sqrt{R}) - I_1(2\sqrt{b}\sqrt{R}) K_1(2\sqrt{b}\sqrt{r_0}),$$

$$\Delta_\mu = I_\mu(2\sqrt{b}\sqrt{r_0}) K_\mu(2\sqrt{b}\sqrt{R}) - I_\mu(2\sqrt{b}\sqrt{R}) K_\mu(2\sqrt{b}\sqrt{r_0}).$$

Принимая во внимание решения (20) и выражения (23), (24) для постоянных $\tilde{C}_1^{(j)}, \tilde{C}_2^{(j)}$ ($j = \overline{0, 1}$), по формуле (2) получим распределение температуры $T(r, \theta)$ в полярно-ортотропной обратноконической кольцевой пластине с учетом теплообмена ее с внешней средой:

$$\begin{aligned} T(r, \theta) = & T_1^* \left(\frac{1}{\Delta_2} \sqrt{\frac{r_0}{r}} \left(I_1(2\sqrt{b}\sqrt{r}) K_1(2\sqrt{b}\sqrt{R}) - I_1(2\sqrt{b}\sqrt{R}) K_1(2\sqrt{b}\sqrt{r}) \right) \right) + \\ & + NT_2^* \left(\frac{1}{\Delta_2} \sqrt{\frac{R}{r}} \left(I_1(2\sqrt{b}\sqrt{r_0}) K_1(2\sqrt{b}\sqrt{r}) - I_1(2\sqrt{b}\sqrt{r}) K_1(2\sqrt{b}\sqrt{r_0}) \right) \right) + \end{aligned}$$

$$\begin{aligned}
 & + T_0 \left(1 + \frac{1}{\Delta_2} \left(\sqrt{\frac{R}{r}} K_1(2\sqrt{b}\sqrt{r_0}) - \sqrt{\frac{r_0}{r}} K_1(2\sqrt{b}\sqrt{R}) \right) I_1(2\sqrt{b}\sqrt{r}) + \right. \\
 & \left. + \frac{1}{\Delta_2} \left(\sqrt{\frac{r_0}{r}} I_1(2\sqrt{b}\sqrt{R}) - \sqrt{\frac{R}{r}} I_1(2\sqrt{b}\sqrt{r_0}) \right) K_1(2\sqrt{b}\sqrt{r}) \right) - \\
 & - NT_2^* \sum_{n=1}^{\infty} \frac{2}{\Delta_2} \sqrt{\frac{R}{r}} \left(I_{\mu}(2\sqrt{b}\sqrt{r}) K_{\mu}(2\sqrt{b}\sqrt{r_0}) - I_{\mu}(2\sqrt{b}\sqrt{r_0}) K_{\mu}(2\sqrt{b}\sqrt{r}) \right) \cos Nn\theta.
 \end{aligned}$$

Коническая кольцевая пластина. Толщина конической кольцевой пластины задается формулой

$$h(r) = h_0^* \left(1 - \frac{r}{R_1} \right), \text{ где } h_0^* = \frac{h_0}{1 - \frac{r_0}{R_1}}, \quad R_1 = \frac{h_0 R - h_1 r_0}{h_0 - h_1}, \quad h_0, h_1 - \text{толщина пластины на внутреннем } (r = r_0)$$

и внешнем контуре ($r = R$) соответственно ($h_1 < h_0$). Дифференцируя функцию $h(r)$ и подставляя в уравнение (6), получим

$$\frac{d^2 \Theta_n^{(1)}}{dr^2} + \left(\frac{1}{r} - \frac{1}{R_1 - r} \right) \frac{d\Theta_n^{(1)}}{dr} - \left(\frac{\lambda_{\theta}}{\lambda_r} \frac{(Nn)^2}{r^2} + \frac{H\sqrt{h_0^{*2} + 4R_1^2}}{\lambda_r h_0^*} \frac{1}{R_1 - r} \right) \Theta_n^{(1)}(r) = 0. \quad (25)$$

Обозначив $\frac{HR_1\sqrt{h_0^{*2} + 4R_1^2}}{\lambda_r h_0^*} = b^*$, $N\sqrt{\frac{\lambda_{\theta}}{\lambda_r}} n = v$ и сделав замену переменной $s = \frac{r}{R_1}$, где $s \in [\delta_0, \delta_1]$,

$\delta_0 = \frac{r_0}{R_1} \geq 0$, $\delta_1 = \frac{R}{R_1} \leq 1$, запишем уравнение (25) в виде

$$s^2(1-s) \frac{d^2 \Theta_n^{(1)}}{ds^2} + (1-2s)s \frac{d\Theta_n^{(1)}}{ds} - (b^*s^2 - v^2s + v^2) \Theta_n^{(1)}(s) = 0. \quad (26)$$

Введем функции $f(s) = 1 - s$, $g(s) = 1 - 2s$, $p(s) = -(b^*s^2 - v^2s + v^2)$ и представим уравнение (26) следующим образом:

$$s^2 f(s) \frac{d^2 \Theta_n^{(1)}}{ds^2} + s g(s) \frac{d\Theta_n^{(1)}}{ds} + p(s) \Theta_n^{(1)}(s) = 0. \quad (27)$$

Точка $s = 0$ является регулярной, так как функции $f(s)$, $g(s)$, $p(s)$ разложимы в степенные ряды в окрестности этой точки и $f(0) \neq 0$. Вид решения уравнения (27) в окрестности точки $s = 0$ зависит от решения определяющего уравнения [6]:

$$\rho(\rho - 1)f(0) + \rho g(0) + p(0) = 0.$$

Подставляя конкретные значения функций $f(0) = 1$, $g(0) = 1$, $p(0) = -v^2$ в определяющее уравнение, получим квадратное уравнение для параметра ρ :

$$\rho^2 - v^2 = 0.$$

Его корни $\rho_1 = v$, $\rho_2 = -v$. Так как разность корней $d = \rho_1 - \rho_2 = 2v$ есть не целое число, то решение дифференциального уравнения (26) представимо в виде

$$\Theta_n^{(1)}(s) = \hat{C}_1^{(1)} \Theta_{n,1}^{(1)}(s) + \hat{C}_2^{(1)} \Theta_{n,2}^{(1)}(s), \quad (28)$$

где $\Theta_{n,1}^{(1)}(s) = s^v \sum_{k=0}^{\infty} c_k^{(1)} s^k$, $\Theta_{n,2}^{(1)}(s) = s^{-v} \sum_{k=0}^{\infty} d_k^{(1)} s^k$ – частные решения уравнения (26); $\hat{C}_1^{(1)}$, $\hat{C}_2^{(1)}$ – произвольные постоянные.

Коэффициенты $c_k^{(1)}$, $d_k^{(1)}$ степенных рядов определяются из рекуррентных соотношений

$$c_{k+1}^{(1)} = \frac{k(k+1) + v(2k+1)}{(k+1)^2 + 2v(k+1)} c_k^{(1)} + \frac{b^*}{(k+1)^2 + 2v(k+1)} c_{k-1}^{(1)}, \quad k \geq 1,$$

$$c_0^{(1)} = 1 + 2\nu, \quad c_1^{(1)} = \nu;$$

$$d_{k+1}^{(1)} = \frac{k(k+1) - \nu(2k+1)}{(k+1)^2 - 2\nu(k+1)} d_k^{(1)} + \frac{b^*}{(k+1)^2 - 2\nu(k+1)} d_{k-1}^{(1)}, \quad k \geq 1,$$

$$d_0^{(1)} = 1 - 2\nu, \quad d_1^{(1)} = -\nu.$$

Постоянные $\hat{C}_1^{(1)}, \hat{C}_2^{(1)}$ найдем из граничных условий. Подставляя найденное решение (28) в граничные условия (10), получим следующую систему алгебраических уравнений относительно неизвестных $\hat{C}_1^{(1)}, \hat{C}_2^{(1)}$:

$$(n \geq 1) \quad \begin{cases} \hat{C}_1^{(1)} \Theta_{n,1}^{(1)}(\delta_0) + \hat{C}_2^{(1)} \Theta_{n,2}^{(1)}(\delta_0) = 0, \\ \hat{C}_1^{(1)} \Theta_{n,1}^{(1)}(\delta_1) + \hat{C}_2^{(1)} \Theta_{n,2}^{(1)}(\delta_1) = 2NT_2^*. \end{cases} \quad (29)$$

Решение системы (29) есть

$$(n \geq 1) \quad \begin{cases} \hat{C}_1^{(1)} = -NT_2^* \frac{2}{\Delta_3^{(n)}} \Theta_{n,2}^{(1)}(\delta_0), \\ \hat{C}_2^{(1)} = NT_2^* \frac{2}{\Delta_3^{(n)}} \Theta_{n,1}^{(1)}(\delta_0), \end{cases}$$

где $\Delta_3^{(n)} = \Theta_{n,1}^{(1)}(\delta_0) \Theta_{n,2}^{(1)}(\delta_1) - \Theta_{n,1}^{(1)}(\delta_1) \Theta_{n,2}^{(1)}(\delta_0)$ – определитель.

Таким образом, решение (28) запишется в виде

$$\Theta_n^{(1)}(s) = -NT_2^* \frac{2}{\Delta_3^{(n)}} \left(\Theta_{n,1}^{(1)}(s) \Theta_{n,2}^{(1)}(\delta_0) - \Theta_{n,1}^{(1)}(\delta_0) \Theta_{n,2}^{(1)}(s) \right). \quad (30)$$

Исходя из решения осесимметричной задачи стационарной теплопроводности [4] и решения (30), по формуле (2) получим распределение температуры $T(s, \theta)$ в полярно-ортотропной конической кольцевой пластине при учете теплообмена с внешней средой:

$$\begin{aligned} T(s, \theta) = & \frac{T_1^*}{\Delta_3^{(0)}} \left(\Theta_0^{(1)}(s) \Theta_0^{(2)}(\delta_1) - \Theta_0^{(1)}(\delta_1) \Theta_0^{(2)}(s) \right) - \frac{NT_2^*}{\Delta_3^{(0)}} \left(\Theta_0^{(1)}(s) \Theta_0^{(2)}(\delta_0) - \Theta_0^{(1)}(\delta_0) \Theta_0^{(2)}(s) \right) + \\ & + T_0 \left(1 + \frac{1}{\Delta_3^{(0)}} \left(\Theta_0^{(2)}(\delta_0) - \Theta_0^{(2)}(\delta_1) \right) \Theta_0^{(1)}(s) - \frac{1}{\Delta_3^{(0)}} \left(\Theta_0^{(1)}(\delta_0) - \Theta_0^{(1)}(\delta_1) \right) \Theta_0^{(2)}(s) \right) - \\ & - NT_2^* \sum_{n=1}^{\infty} \frac{2}{\Delta_3^{(n)}} \left(\Theta_{n,1}^{(1)}(s) \Theta_{n,2}^{(1)}(\delta_0) - \Theta_{n,1}^{(1)}(\delta_0) \Theta_{n,2}^{(1)}(s) \right) \cos Nn\theta, \end{aligned}$$

где $\Theta_0^{(1)}(s) = \sum_{k=0}^{\infty} a_k s^k$, $\Theta_0^{(2)}(s) = \left(\sum_{k=0}^{\infty} a_k s^k \right) \ln s + \sum_{k=0}^{\infty} b_k s^k$ – частные решения дифференциального уравнения осесимметричной стационарной задачи теплопроводности для профилированных полярно-ортотропных кольцевых пластин с учетом теплообмена с внешней средой, коэффициенты a_k, b_k определяются из рекуррентных соотношений [4]; $\Delta_3^{(0)} = \Theta_0^{(1)}(\delta_0) \Theta_0^{(2)}(\delta_1) - \Theta_0^{(1)}(\delta_1) \Theta_0^{(2)}(\delta_0)$ – определитель.

Профилированные анизотропные кольцевые пластины. Для всех остальных полярно-ортотропных кольцевых пластин переменной толщины общее решение уравнения (6) будем находить с помощью решения соответствующего линейного интегрального уравнения Вольтерры 2-го рода. Полагаем

$$\frac{d^2 \Theta_n^{(1)}}{dr^2} = \eta_n^{(1)}(r). \quad (31)$$

Последовательно интегрируя соотношение (31), имеем

$$\frac{d\Theta_n^{(1)}}{dr} = \int_{r_0}^r \eta_n^{(1)}(s) ds + \dot{\Theta}_n^{(1)}(r_0), \quad \Theta_n^{(1)}(r) = \int_{r_0}^r (r-s) \eta_n^{(1)}(s) ds + \dot{\Theta}_n^{(1)}(r_0)(r-r_0) + \Theta_n^{(1)}(r_0). \quad (32)$$

При выводе выражений (32) использовалась знаменитая формула Дирихле [7; 8]:

$$\int_{r_0}^r dr_1 \int_{r_0}^{r_1} dr_2 \dots \int_{r_0}^{r_{n-1}} f(r_n) dr_n = \frac{1}{(n-1)!} \int_{r_0}^r (r-s)^{n-1} f(s) ds.$$

Подстановка в уравнение (6) вместо функции $\Theta_n^{(1)}(r)$ и ее производных правых частей выражений (31), (32) приводит к линейному интегральному уравнению Вольтерры 2-го рода для разрешающей функции $\eta_n^{(1)}(r)$:

$$\eta_n^{(1)}(r) = \lambda \int_{r_0}^r K_n(r, s) \eta_n^{(1)}(s) ds + f_n^{(1)}(r), \quad (33)$$

где $\lambda = -1$ есть числовой параметр; $K_n(r, s) = \frac{h'(r)}{h(r)} + \frac{1}{r} - \left(\frac{\lambda_\theta (Nn)^2}{\lambda_r r^2} + \frac{H}{\lambda_r} \sqrt{\frac{4}{h^2(r)} + \left(\frac{h'(r)}{h(r)} \right)^2} \right) (r-s) -$

ядро интегрального уравнения; $f_n^{(1)}(r) = \frac{\partial K_n(r, s)}{\partial s} \Theta_n^{(1)}(r_0) - K_n(r, r_0) \dot{\Theta}_n^{(1)}(r_0) -$ свободный член интегрального уравнения.

Запишем в явном виде ядра интегрального уравнения (33) для полярно-ортотропных кольцевых пластин степенного и экспоненциального профилей.

Толщина кольцевой пластины степенного профиля задается формулой $h(r) = h_0 \left(\frac{r_0}{r} \right)^\alpha$, $\alpha \in \mathbb{R} \setminus \{-1; 0\}$,

где h_0 – толщина пластины на внутреннем контуре ($r = r_0$). Ядро интегрального уравнения (33) в данном случае есть

$$K_n^{\text{ст}}(r, s) = \frac{1-\alpha}{r} - \left(\frac{\lambda_\theta (Nn)^2}{\lambda_r r^2} + \frac{2H}{\lambda_r h_0} \sqrt{\frac{\alpha^2}{4} \left(\frac{h_0}{r_0} \right)^2 \left(\frac{r_0}{r} \right)^2 + \left(\frac{r_0}{r} \right)^{-2\alpha}} \right) (r-s).$$

Для кольцевой пластины экспоненциального профиля, толщина которой описывается формулой

$$h(r) = h_0 e^{\beta \left(\frac{r-r_0}{R} \right)}, \quad \text{где } \beta = \frac{\ln \left(\frac{h_1}{h_0} \right)}{1 - \frac{r_0}{R}}, \quad h_0, h_1 - \text{толщина пластины на внутреннем } (r = r_0) \text{ и внешнем контуре } (r = R) \text{ соответственно } (h_1 < h_0),$$

ядро интегрального уравнения (33) есть

$$K_n^{\text{эксп}}(r, s) = \frac{\beta}{R} + \frac{1}{r} - \left(\frac{\lambda_\theta (Nn)^2}{\lambda_r r^2} + \frac{2H}{\lambda_r h_0^*} \sqrt{\frac{1}{4} \left(\beta \frac{h_0^*}{R} \right)^2 + e^{-2\beta \left(\frac{r}{R} \right)}} \right) (r-s).$$

Общее решение линейного интегрального уравнения Вольтерры 2-го рода (33) записывается с помощью *резольвенты* $R_n(r, s; \lambda)$ в виде [7]

$$\eta_n^{(1)}(r) = \lambda \int_{r_0}^r R_n(r, s; \lambda) f_n^{(1)}(s) ds + f_n^{(1)}(r). \quad (34)$$

Здесь функция $R_n(r, s; \lambda)$ определяется функциональным рядом, а именно

$$R_n(r, s; \lambda) = \sum_{m=0}^{\infty} \lambda^m K_{n, m+1}(r, s),$$

который для непрерывных ядер $K_{n, m}(r, s)$ сходится абсолютно и равномерно.

Повторяющиеся, или итерированные, ядра $K_{n, m}(r, s)$ вычисляются по рекуррентным формулам

$$\begin{aligned} K_{n,1}(r, s) &= K_n(r, s), \\ K_{n,2}(r, s) &= \int_s^r K_n(r, t) K_{n,1}(t, s) dt, \\ &\dots\dots\dots \\ K_{n,m}(r, s) &= \int_s^r K_n(r, t) K_{n,m-1}(t, s) dt. \end{aligned}$$

Если свободный член $f_n^{(1)}(r)$ непрерывен на отрезке $[r_0, R]$, а ядро $K_n(r, s)$ непрерывно при $r_0 \leq r \leq R$, $r_0 \leq s \leq r$, то линейное интегральное уравнение Вольтерры 2-го рода (33) имеет при любом параметре λ ($\lambda \neq 0$) единственное непрерывное решение, определяемое формулой (34).

Из-за наличия иррациональностей в ядрах интегральных уравнений для пластин со степенным и экспоненциальным профилями вычисление интегралов итерированных ядер следует вести численными методами.

Отметим, что интегральные уравнения Вольтерры 2-го рода можно решать и другими аналитическими и численными методами, указанными, например, в [8].

Применяя вторую формулу из (32) и граничные условия (10), запишем общее решение уравнения (6) через разрешающую функцию $\eta_n^{(1)}(r)$:

$$\Theta_n^{(1)}(r) = \int_{r_0}^r (r-s) \eta_n^{(1)}(s) ds - \frac{r-r_0}{R-r_0} \int_{r_0}^R (R-s) \eta_n^{(1)}(s) ds + 2NT_2^* \frac{r-r_0}{R-r_0}. \quad (35)$$

Используя решение осесимметричной задачи теплопроводности из [4], решение (35) и разложение (4), по формуле (2) получим следующее распределение температуры $T(r, \theta)$ в профилированной полярно-ортотропной кольцевой пластине с учетом теплообмена с внешней средой:

$$\begin{aligned} T(r, \theta) &= \int_{r_0}^r (r-s) \eta_0(s) ds - \frac{r-r_0}{R-r_0} \int_{r_0}^R (R-s) \eta_0(s) ds + T_1^* \frac{R-r}{R-r_0} + NT_2^* \frac{r-r_0}{R-r_0} + \\ &+ \sum_{n=1}^{\infty} \left(\int_{r_0}^r (r-s) \eta_n^{(1)}(s) ds - \frac{r-r_0}{R-r_0} \int_{r_0}^R (R-s) \eta_n^{(1)}(s) ds + 2NT_2^* \frac{r-r_0}{R-r_0} \right) \cos n\theta. \end{aligned}$$

Заключение

Найденные точные аналитические решения неосесимметричной стационарной задачи теплопроводности для трех профилей анизотропных кольцевых пластин (постоянной толщины, обратноконической и конической) будут применены при расчете неосесимметричных температурных напряжений для указанных пластин в наших следующих работах аналогично проведенным ранее расчетам осесимметричных температурных напряжений для анизотропных кольцевых пластин переменной толщины [9; 10]. В случае использования в машиностроительных или авиационных конструкциях анизотропных кольцевых пластин с более сложным профилем для расчета температур в них надо применить более общую формулу (36) с численным решением интегральных уравнений Вольтерры 2-го рода.

Библиографические ссылки

1. Королевич ВВ, Медведев ДГ. Решение неосесимметричной стационарной задачи теплопроводности для полярно-ортотропной кольцевой пластины переменной толщины с теплоизолированными основаниями. *Журнал Белорусского государственного университета. Математика. Информатика*. 2018;1:77–87.
2. Уздалев АИ. *Некоторые задачи термоупругости анизотропного тела*. Саратов: Издательство Саратовского государственного университета; 1967. 168 с.
3. Уздалев АИ, Брюханова ЕН. Уравнение теплопроводности для пластин переменной толщины с неоднородными теплофизическими свойствами. В: Уздалев АИ, редактор. *Задачи прикладной теории упругости*. Саратов: Саратовский политехнический институт; 1985. с. 3–7.
4. Королевич ВВ. Стационарные температурные поля в анизотропных кольцевых пластинах переменной толщины с учетом теплообмена с внешней средой. *Журнал Белорусского государственного университета. Математика. Информатика*. 2018;2:58–66.
5. Бронштейн ИН, Семендяев КА. *Справочник по математике для инженеров и учащихся ВТУЗов*. Москва: Наука; 1981. 721 с.

6. Камке Э. *Справочник по обыкновенным дифференциальным уравнениям*. Москва: Наука; 1976. 576 с.
7. Краснов МЛ, Киселев АИ, Макаренко ГИ. *Интегральные уравнения: задачи и примеры с подробными решениями*. Москва: КомКнига; 2007. 192 с.
8. Верлань АФ, Сизиков ВС. *Интегральные уравнения: методы, алгоритмы, программы*. Киев: Наукова думка; 1986. 543 с.
9. Королевич ВВ, Медведев ДГ. Решение осесимметричной плоской задачи термоупругости для вращающегося в тепловом поле полярно-ортотропного диска переменной толщины методом интегрального уравнения Вольтерры второго рода. *Журнал Белорусского государственного университета. Математика. Информатика*. 2017;1:47–52.
10. Королевич ВВ, Медведев ДГ. Расчет осесимметричного термосилового изгиба вращающегося в тепловом поле полярно-ортотропного диска переменной толщины методом интегрального уравнения Вольтерры второго рода. *Журнал Белорусского государственного университета. Математика. Информатика*. 2017;2:44–51.

References

1. Karalevich UV, Medvedev DG. The solution of the nonaxisymmetric stationary problem of heat conduction for the polar-orthotropic annular plate of variable thickness with thermal insulated bases. *Journal of the Belarusian State University. Mathematics and Informatics*. 2018;1:77–87. Russian.
2. Uzdalev AI. *Nekotorye zadachi termouprugosti anizotropnogo tela* [Some problems of thermoelasticity of an anisotropic body]. Saratov: Izdatel'stvo Saratovskogo gosudarstvennogo universiteta; 1967. 168 p. Russian.
3. Uzdalev AI, Bryukhanova EN. Equations of thermal conductivity for plates of variable thickness with inhomogeneous thermophysical properties. In: Uzdalev AI, editor. *Zadachi prikladnoi teorii uprugosti* [Problems of applied theory of elasticity]. Saratov: Saratovskii politekhnicheskii institut; 1985. p. 3–7. Russian.
4. Karalevich UV. Stationary temperature fields in the anisotropic ring plates of variable thickness considering the heat exchange with external environment. *Journal of the Belarusian State University. Mathematics and Informatics*. 2018;2:58–66. Russian.
5. Bronshtein IN, Semendiaev KA. *Spravochnik po matematike dlya inzhenerov i uchashchikhsya VTUZov* [A handbook on mathematics for engineers and students VTUZov]. Moscow: Nauka; 1981. 721 p. Russian.
6. Kamke E. *Differentialgleichungen. Lösungsmethoden und Lösungen. I. Gewöhnliche Differentialgleichungen*. Leipzig: Akademische Verlagsgesellschaft Becker & Erler; 1942. XXVI + 642 S.
Russian edition: Kamke E. *Spravochnik po obyknovennym differentsial'nym uravneniyam* [Handbook of ordinary differential equations]. Moscow: Nauka; 1976. 576 p.
7. Krasnov ML, Kiselev AI, Makarenko GI. *Integral'nye uravneniya: zadachi i primery s podrobnymi resheniyami* [Integral equations: problems and examples with detailed solutions]. Moscow: KomKniga; 2007. 192 p. Russian.
8. Verlan AF, Sizikov VS. *Integral'nye uravneniya: metody, algoritmy, programmy* [Integral equations: methods, algorithms, programs]. Kyiv: Naukova dumka; 1986. 543 p. Russian.
9. Karalevich UV, Medvedev DG. Solution of the axisymmetric plane thermoelasticity problem for a polar-orthotropic disc of variable thickness in the rotating thermal field by Volterra integral equation of the second kind. *Journal of the Belarusian State University. Mathematics and Informatics*. 2017;1:47–52. Russian.
10. Karalevich UV, Medvedev DG. Calculation of the axisymmetric thermopower bending problem of rotating in the thermal field of the polar-orthotropic disc with variable thickness by Volterra integral equation of the second kind. *Journal of the Belarusian State University. Mathematics and Informatics*. 2017;2:44–51. Russian.

Статья поступила в редколлегию 29.01.2020.
Received by editorial board 29.01.2020.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ

THEORETICAL FOUNDATIONS OF COMPUTER SCIENCE

УДК 004.942

ПРИМЕНЕНИЕ ФОРМАЛЬНЫХ МЕТОДОВ ПРИ ПРОЕКТИРОВАНИИ КОЛЛАБОРАЦИОННОЙ СИСТЕМЫ ПРОТИВОВИРУСНОЙ ЗАЩИТЫ

Р. Е. ШАРЫКИН¹⁾, А. Н. КУРБАЦКИЙ¹⁾

¹⁾Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь

Предлагается подход, позволяющий исследовать математическую модель системы защиты от вирусов на этапе ее проектирования с помощью статистического анализа исполняемой спецификации модели, основанной на формализме распределенных объектно ориентированных стохастических гибридных систем (РООГС). Важными аспектами модели являются ее распределенный и вероятностный характер. Эти аспекты делают модель более сложной для проведения атак, но в то же время значительно усложняют понимание ее свойств разработчиком. На данном примере мы показываем, как с помощью использования спецификации системы в качестве модели РООГС вкупе со статистическим анализом можно исследовать ее свойства на раннем этапе проектирования и как с применением данного подхода можно обнаружить «дефекты» модели и исправить их еще в процессе ее создания.

Ключевые слова: математическое моделирование; гибридные системы; стохастические системы; спецификация моделей; совместная антивирусная защита.

Образец цитирования:

Шарыкин РЕ, Курбацкий АН. Применение формальных методов при проектировании коллаборационной системы противовирусной защиты. *Журнал Белорусского государственного университета. Математика. Информатика.* 2020;1: 59–69.
<https://doi.org/10.33581/2520-6508-2020-1-59-69>

For citation:

Sharykin RE, Kourbatski AN. Application of formal methods in the design of a collaborative virus defense system. *Journal of the Belarusian State University. Mathematics and Informatics.* 2020;1:59–69. Russian.
<https://doi.org/10.33581/2520-6508-2020-1-59-69>

Авторы:

Роман Евгеньевич Шарыкин – соискатель кафедры технологий программирования факультета прикладной математики и информатики. Научный руководитель – А. Н. Курбацкий.

Александр Николаевич Курбацкий – доктор технических наук, профессор; заведующий кафедрой технологий программирования факультета прикладной математики и информатики.

Authors:

Roman E. Sharykin, competitor at the department of software engineering, faculty of applied mathematics and computer science.
sharykin@gmail.com

Alexander N. Kourbatski, doctor of science (engineering), full professor; head of the department of software engineering, faculty of applied mathematics and computer science.
kurb@unibel.by

APPLICATION OF FORMAL METHODS IN THE DESIGN OF A COLLABORATIVE VIRUS DEFENSE SYSTEM

R. E. SHARYKIN^a, A. N. KOURBATSKI^a

^aBelarusian State University, 4 Niezaliežnasci Avenue, Minsk 220030, Belarus

Corresponding author: R. E. Sharykin (sharykin@gmail.com)

This article proposes an approach that allows us to study a mathematical model of a virus protection system at the stage of its design using statistical analysis of an executable model specification based on the formalism of Distributed Object Based Stochastic Hybrid Systems (DOBSHS). Important aspects of the model are its distributed and probabilistic nature. These aspects make the model more difficult to carry out attacks, but at the same time significantly complicate the understanding of its properties by the developer. In this example, we show how, using the specification of the system as a DOBSHS model, coupled with its statistical analysis, we can investigate its properties at an early stage of design and how, using this approach, we can detect «defects» of the model and correct them during the process of creating the model.

Keywords: mathematical modeling; hybrid systems; stochastic systems; model specification; collaborative virus defense.

Введение

Ввиду растущей важности и сложности распределенных систем вирусной защиты использование формальных методов для понимания динамики таких систем на ранних этапах их разработки представляется важной задачей. Одной из трудностей применения формальных методов в данной области является определение подходящей формальной модели, такой как сети Петри или дискретная марковская цепь. После того как выбор формальной модели был сделан, может быть очень затратным ее изменение впоследствии в случае, если обнаружено, что другая формальная модель лучше подходит для описания рассматриваемой системы.

Цель настоящей статьи – изложение подхода к разработке модели сложных динамических распределенных стохастических систем с коммуникацией на ранних этапах до проведения ее аналитического анализа и его иллюстрация на примере предварительной модели стохастической групповой системы защиты от вирусов и экспериментов с ней.

Мы представляем подход к применению формальных методов на ранних этапах дизайна системы защиты от вирусов, основанный на использовании формальной модели распределенных объектно ориентированных стохастических гибридных систем (РООСГС) [1], и подход к ее верификации, изложенный в [2]. Данная модель базируется на переписывающей логике [3]. Использование таковой позволяет применять формальные методы в начале проектирования, в то же время не ограничивая разработчика определенным формализмом. Показано, что различные математические модели могут быть естественным образом представлены с помощью переписывающей логики [3; 4], а основанный на ней формализм может быть сжатым, интуитивно понятным и хорошо подходит для спецификации распределенных параллельных систем с асинхронной коммуникацией. Спецификации, выполненные в переписывающей логике, могут выполняться с помощью системы Maude [5], которая позволяет симулировать и улучшать спецификацию системы защиты для различных сценариев атак в самом начале разработки системы защиты. Как только разработчик остается удовлетворенным полученной спецификацией, он может выбрать наиболее подходящую математическую модель с известным представлением в переписывающей логике для формального доказательства критически важных свойств системы либо нахождения более сложных недостатков, которые невозможно выявить с помощью техники симуляций. Maude также предоставляет средства, облегчающие проведение доказательств в формализме переписывающей логики [6].

После того как формализм выбран, важным вопросом является анализ системы на ранних этапах ее разработки. Желаемый метод должен быть «легким» в том смысле, что он может давать возможность разработчику концентрироваться на алгоритме защиты и его параметрах. Мы предлагаем способ, который предоставляет возможность получать быструю оценку основных поведенческих свойств системы и испробовать модель защиты на различных предположениях относительно окружения, позволяя потратить усилия для проведения более сложных формальных процедур валидации на поздних этапах, когда пространство возможностей для дизайна уже сокращено.

Для демонстрации нашей методологии рассматривается частный случай вероятностного алгоритма защиты от вирусов. В примере системы защиты от вирусных атак предлагается подход [2], основанный на

симуляциях модели и использующий язык QuaTE_x [7] для задания свойств, подлежащих изучению. Данный подход эффективен для количественного исследования стохастических систем, таких как протоколы защиты от нежелательного проникновения при распределенных атаках. Представлен формальный подход к анализу поведенческих свойств системы, распределенной по узлам в контексте защиты от вирусных атак, и иллюстрируются типы свойств систем защиты, которые применимы как к нашей, так и к другим системам и для которых формальный анализ представляется важным аналитическим методом.

Пример коллаборационной стохастической системы защиты от вирусных атак

Рассматриваемый пример системы защиты от вирусных атак базируется на коллаборационной системе, не являющейся стохастической, которая описана в [8], где детально представлен изначальный алгоритм, обсуждается его эффективность и т. п.

В случае совместной защиты от вирусных атак локальные сети сотрудничают, объединяясь в группы, в которых исходящие маршрутизаторы информируют своих партнеров посредством локальных оповещений о возможной вирусной активности. Если узел получает подобные коллаборационные извещения от N или более источников, он переходит в защитный фильтрующий режим. Алгоритм имеет схожие черты с алгоритмами одноранговых оповещений, представленными в [9; 10], однако в нашем случае распространением оповещений управляет система ограничения скорости соединений, аналогичная описанной в [11]. Эта система распространяет оповещение, когда обнаруживает, что некоторый внутренний узел создает соединения с частотой, превышающей некоторое пороговое значение. Образованные с превышением данного порога соединения с новыми узлами сбрасываются исходящим маршрутизатором до следующего временного периода. Одним из достоинств данной комбинированной стратегии защиты является то, что системы ограничения скорости, распространяющие оповещения, эффективно снижают скорость распространения вируса, позволяя стратегии коллаборации узлов начать действовать, в то время как алгоритмы, основанные на простом обмене оповещениями между узлами, уязвимы для быстро распространяющихся вирусов.

При получении достаточного количества коллаборационных оповещений о вирусной атаке исходящий маршрутизатор имеет возможность переходить в режим защиты, в котором он сбрасывает все пакеты, которые, как предполагается, имеют отношение к большинству оповещений. Для создания достаточно абстрактной модели мы не уточняем, как именно организуется фильтрация, а полагаем, что алгоритм содержит фильтрацию и узлы могут находиться в данном режиме. Существуют основанные на генерации сигнатур исследования по разработке автоматических систем, таких как EarlyBird [12] и Autograph [13], которые могут быть использованы для реализации фильтрации в рассматриваемой нами системе.

Размер групп оповещения существенно влияет на свойства изучаемой модели. Его увеличение приводит к большему подавлению распространения вируса. Однако с ростом размера групп также повышается «цена» обработки оповещений, отправленных в результате ложноположительного обнаружения вируса (более подробное исследование влияния размера групп см. в [10]).

Мы вводим в систему защиты из [8] вероятности обнаружения вируса и ложноположительного обнаружения вируса. Также фазы системы мы заменяем на процессы, которые протекают асинхронно с интервалами, имеющими экспоненциальное распределение. Это делает систему более реалистичной, но в то же время стохастической по своей природе. Основным же дополнением к указанной системе является формирование групп оповещения в соответствии со случайным распределением, в отличие от фиксированных групп в [8]. Структура групп в [8] позволяла провести атаку с полным заражением системы, основываясь на алгоритме формирования групп [14]. При их случайном формировании атаки подобного типа становятся невозможными, так как идея построения атаки критически зависит от способности атакующего предсказать точный состав групп оповещения.

Мы моделируем локальную сеть как граф локальных узлов с одним исходящим маршрутизатором. Несколько локальных сетей объединяются друг с другом посредством их исходящих маршрутизаторов. В целом система групповой защиты моделируется как параллельное, асинхронное развертывание алгоритма защиты локальной сети, установленного на всех исходящих маршрутизаторах. В каждом экземпляре системы защиты локальной сети независимо от других выполняются три процесса (с интервалами запуска, распределенными экспоненциально): детектирование инфекции, формирование группы оповещения, оповещение. Также на всех временных интервалах происходит обновление состояния защиты для каждого экземпляра системы.

При выполнении детектирования исходящий маршрутизатор может наблюдать локальное превышение заданных порогов на скорость установки соединений в некоторых узлах, генерируя локальное оповещение для каждого превышения.

Для формирования групп оповещения исходящий маршрутизатор создает группы размера G из множества участвующих локальных сетей в соответствии с определенным вероятностным распределением.

При выполнении оповещения исходящий маршрутизатор направляет оповещение в свою группу оповещения в случае, если он сгенерировал как минимум одно локальное оповещение к данному моменту. Исходящий маршрутизатор также получает оповещения от других локальных сетей и увеличивает уровень локальной метрики оповещений `alert`, основываясь на количестве полученных локальных оповещений и оповещений от других сетей. Каждое оповещение увеличивает значение `alert` с учетом параметра `severity`, который задает критичность оповещений. Параметр `alert` уменьшается со временем с заранее данной скоростью. Когда `alert` превышает пороговое значение `alpha`, исходящий маршрутизатор применяет фильтрацию ко всем входящим пакетам, которые подпадают под критерий фильтрации. Параметр `alpha` вычисляется как `severity * r`, где `r` обозначает меру коллаборации, необходимую для включения фильтров. Данное фильтрующее состояние сохраняется до тех пор, пока параметр `alert` не достигнет нулевого значения вследствие его уменьшения с течением времени.

Спецификация системы защиты в переписывающей логике

В данном разделе представим спецификацию с помощью переписывающей логики вероятностной групповой системы защиты от компьютерных вирусов, описанной в разделе «Пример коллаборационной стохастической системы защиты от вирусных атак». Для моделирования системы защиты мы используем модель спецификации SHYMaude [2]. Опишем ключевые элементы SHYMaude, имеющие отношение к данному моделированию.

Распределенная конфигурация системы моделируется как множество объектов и сообщений, действующих параллельно в соответствии с множеством правил перезаписи, описывающих поведение отдельных элементов. Объекты в SHYMaude представляются с помощью следующего синтаксиса:

```
< id : C | attr_1: value_1, ..., attr_N: value_N >
```

Здесь `id` – идентификатор объекта; `C` – его класс; `attr_1, ..., attr_N` – имена атрибутов объекта; `value_1, ..., value_N` – значения атрибутов. Пример объекта, представляющего собой узел сети (к примеру, компьютер в сети), выглядит таким образом:

```
< 7 : Node | infected: true, alerts: 5, alert: 2 >
```

Данный узел является инфицированным и имеет уровень `alert`, равный 2.

Активное сообщение для объекта с идентификатором `id` выглядит так:

```
< id <- message >
```

Здесь `message` состоит из множества атрибутов, один из которых может быть выделенным и задавать «команду» для получающего узла (необязательный в случае, если значение сообщения уникально в его отсутствии). Пример сообщения, передающего группу оповещения узлу 7:

```
< 7 <- group : [1, 4, 7] >
```

В этом сообщении `[1, 4, 7]` – множество идентификаторов объектов, составляющих группу оповещения.

Запланированное сообщение задается в виде

```
[time, msg]
```

Здесь `time` – оставшееся время до активации сообщения; `msg` – запланированное сообщение.

Полная спецификация системы с помощью языка SHYMaude может быть найдена в [15]. Для наглядности приведем некоторые переписывающие правила.

Динамика инфицирования системы вирусом описывается следующими переписывающими правилами.

1. Распространение вируса узлом, не находящимся в состоянии фильтрации:

```
rl < id : Node | infected : true, filtering : false, attrSet >  
  < id <- propagate >  
  =>  
  < id : Node | infected : true, filtering : false, attrSet >  
  < (id + 1 + sampleNat(N - 1)) rem N <- infect >  
  [D, < id <- propagate >] with probability D := Exponential(propagateRate).
```

При получении сообщения `propagate` узел производит попытку инфицирования случайно выбранного узла и планирует следующую попытку через случайный интервал времени, выбранный в соответствии

с экспоненциальным распределением, определяемым параметром `propagateRate`. Атрибут `attrSet` является переменной типа `AttributeSet`, которая для данного переписывающего правила может быть равна любому набору пар атрибутов и их значений объекта.

2. Получение команды `propagate` узлом в состоянии фильтрации:

```
rl < id : Node | infected : true, filtering : true, attrSet >
  < id <- propagate >
  =>
  < id : Node | infected : true, filtering : true, attrSet >
  [D, < id <- propagate >] with probability D := Exponential(propagateRate).
```

Указанный узел не может заражать другие узлы и лишь планирует следующую попытку.

3. Получение команды инфицирования (попытки инфицирования данного узла):

```
rl < id : Node | infected : false, filtering : false, attrSet >
  < id <- infect > =>
  < id : Node | infected : true, filtering : false, attrSet >
  [D, < id <- propagate >] with probability D := Exponential(propagateRate).
```

Не находящийся в состоянии фильтрации узел, получивший свидетельствующее о попытке инфицирования сообщение `infect`, инфицируется и планирует попытку заражения.

4. Получение команды инфицирования инфицированным узлом:

```
rl < id : Node | infected : true, filtering : false, attrSet > < id <- infect >
  =>
  < id : Node | infected : true, filtering : false, attrSet >.
```

Если узел уже инфицирован, то попытка его инфицирования не изменяет его состояния.

5. Получение команды инфицирования узлом, находящимся в состоянии фильтрации:

```
rl < id : Node | filtering : true, attrSet > < id <- infect >
  =>
  < id : Node | filtering : true, attrSet >.
```

Указанный узел не может быть инфицирован.

Динамика системы защиты описывается следующими правилами.

6. Детектирование вируса:

```
rl < id : Node | infected : infected, detected : detected, attrSet >
  < id <- detect >
  =>
  < id : Node | infected : infected, detected : if infected then D else F fi, attrSet >
  with probability D := Bernoulli(detectionProb), F := Bernoulli(fpRate)
  [D, < id <- detect >] with probability D := Exponential(detectRate).
```

В этом правиле происходит детектирование вируса с заданной вероятностью, также учтена ложноположительная вероятность обнаружения вируса. Детектирование производится через случайные промежутки времени, распределенные экспоненциально.

7. Оповещение групп:

```
rl < id : Node | infected : infected, detected : detected, group : group, attrSet >
  < id <- alertGroup >
  =>
  if(detected) then sendGroupAlerts(group) else none fi
  < id : Node | infected : infected, detected : detected, group : group, attrSet >
  [D, < id <- alertGroup >] with probability D := Exponential(alertRate).
```

Оповещение производится только узлами, которые детектировали вирус.

8. Получение оповещения:

```
rl < id : Node | alerts : alerts, attrSet >
  < id <- alert >
  =>
  < id : Node | alerts : alerts + 1, attrSet >
```

При получении оповещения узел увеличивает счетчик оповещений на единицу.

Метрики оценки систем защиты

Оценка и сравнение большого количества подходов к защите от вирусов являются задачей современных исследований. В обзоре [16], анализирующем текущее состояние разработок в области формализации оценок и сравнительных критериев, отмечено, что оценка противовирусных стратегий часто основывается исключительно на том, как влияет защита на темп роста инфекции. Однако во многих случаях это лишь одна из метрик, и она не позволяет различать схемы защиты, похожие на конкретно выбранной метрике.

В [16] предлагаются дополнительные метрики, которые дают более глубокое понимание различия поведения систем защиты и предоставляют возможность сравнивать эти системы в измерениях, отличных от темпов роста инфекции. Такие метрики позволяют оценивать системы защиты, учитывая их особенности, например возможность своевременной интервенции человека или нежелательность нахождения большей части системы в режиме фильтрации, так как последняя может оказать серьезный эффект на производительность. В качестве простого примера метрики, иллюстрирующей вторую особенность, приведем процент незараженных узлов, находящихся в режиме без фильтрации после достижения верхнего предела заражения системы (далее будем говорить также, что система достигла насыщения). Эта метрика может быть очень важным аспектом при сравнении различных систем, так как она дает количественную оценку части системы, которая сохранила максимальную производительность после того, как дальнейшее прогрессирование распространения вируса более не ожидается, иными словами, вирус достиг своего полного насыщения.

Представим более подробно четыре метрики – три из них связаны с кривой заражения и одна не связана с ней.

Рассмотрим тип кривой распространения вируса, который реализуется при симуляциях системы защиты, описанной в данной статье. Форма кривой является сигмовидной, с резким ростом вначале и последующими достижением равновесия и остановкой эпидемии. Визуально можно выделить три величины, которые характеризуют этот тип кривых: процент зараженных узлов при насыщении, максимальная скорость распространения инфекции и время, за которое достигается насыщение.

Метрика 1. Процент зараженных хостов после того, как вирус достиг полного насыщения.

Метрика 2. Максимальная скорость распространения вируса, измеренная как процент заразившихся узлов в период, соответствующий пику заражения.

Метрика 3. Временная точка, в которой вирус достигает своего полного насыщения.

Большинство оценок, используемых при проектировании систем защиты от вирусов, основываются на влиянии этих систем на распространение вируса. Это дает прямое представление об общей эффективности системы, но не учитывает цену применяемых элементов защиты. Такая цена может выражаться в падении общей производительности из-за необходимости фильтрации, усложнении коммуникации, эффектах на локальную защиту для участвующих и не участвующих сетей. Приведем пример метрики, дающей количественное представление о части системы, не затронутой эффектами системы защиты.

Метрика 4. Количество неинфицированных узлов, находящихся в режиме без защиты, после того как вирус достиг своего полного насыщения.

Данную метрику дополнительно можно использовать для оценки эффективности системы.

Статистический анализ

Спецификацию в SHYMaude можно легко транслировать в спецификацию Maude [2], являющуюся выполняемой логической спецификацией [5]. Для анализа системы используем инструмент MultiVeStA [17], который, в свою очередь, основан на инструментах VeStA [7] и PVeStA [18]. MultiVeStA предлагает простую и понятную интеграцию существующих дискретно-событийных симуляторов, язык MultiQuaTEх (расширение языка QuaTEх [7]), который позволяет более компактное задание свойств систем, и клиент-серверную архитектуру для воспроизведения распределенных симуляций. Для анализа MultiVeStA использует статистический метод Монте-Карло. С помощью инструмента можно достигать предустановленного уровня точности результата. Также в системе возможны распределенные вычисления, основанные на клиент-серверном взаимодействии.

Точность результата в MultiVeStA задается с помощью параметров α и δ . Для полученного значения v при использовании данного алгоритма доверительный интервал имеет вид

$$\left[v(1 - \delta), \frac{v}{1 - \delta} \right].$$

Мы использовали величины $\alpha = 0,01$ и $\delta = 0,05$. Выбор параметра α гарантирует, что повторно вычисленные значения будут находиться в доверительном интервале с вероятностью 99 %.

К параметрам системы защиты также относятся количество исходящих узлов, размер группы, метрики строгости и сотрудничества. Эти параметры, а также параметры ложноположительного и ложноотрицательного темпов обнаружения вируса за интервал времени в использованном распределении Бернулли приведены в таблице.

Параметры модели
Model parameters

Параметры	Описание	Значение
N	Количество узлов	20
G	Размер группы	8
severity	Критичность	3
r	Сотрудничество	2
$\alpha = \text{severity} * r$	Порог количества оповещений	6
p_{fp}	Ложноотрицательный темп обнаружения	0,1
p_{fn}	Ложноположительный темп обнаружения	0,05
t_s	Количество временных шагов до объявления насыщения	10

Насыщение распространения вируса было определено как стабильность процента зараженных узлов на протяжении 10 временных шагов.

Распространение вируса с течением времени. Начнем исследование системы с построения графика распространения вируса с течением времени. Используем следующее MultiQuaTEх-выражение для расчета процента зараженных узлов после определенного числа временных интервалов x :

```
MyProperty(x) = if {s.rval(1) >= x} then {s.rval(11)} else # MyProperty({x}) fi;
eval parametric(E[MyProperty(x)], x, 0.0, 1.0, 50.0);
```

где x варьируется от 0 до 50 с шагом 1. По вычисленным для каждого x значениям MultiVeStA строит график.

Здесь и далее QuaTEх-выражения будут приводиться так, как они представляются в MultiVeStA. Выражение $s.rval(n)$ обозначает функцию на состоянии с параметром n , т. е. для каждого n можно задать некоторую функцию на состоянии. Принято использовать $s.rval(1)$ как функцию, возвращающую текущее время. В примере выше $s.rval(11)$ возвращает процент зараженных узлов.

По окончании вычислений, когда достигнут заданный уровень точности, MultiVeStA выводит численные результаты и построенный по ним график (рис. 1).

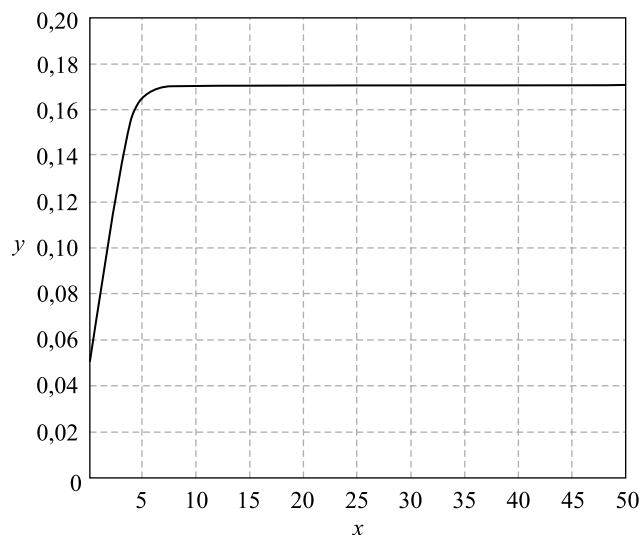


Рис. 1. Распространение вируса

Fig. 1. Virus propagation

Как видно из графика, распространение вируса быстро растет в течение 5 временных интервалов и достигает насыщения примерно после 10 таких интервалов. Пораженной оказывается менее 20 % системы, поэтому можно утверждать, что на заданных параметрах система статистически устойчива к этому типу вируса, если под статистической устойчивостью понимать факт того, что определенная существенная часть системы остается незараженной после достижения насыщения распространения вируса.

Процент зараженных хостов по достижении насыщения. Получим оценку значения метрики 1. MultiQuaTEx-выражение для вычисления этой оценки выглядит следующим образом:

```
percentInfectedAfterSaturation(percentage, count) =  
  if {count <= 0.0} then {s.rval(11)} else  
    if {s.rval(11) >= percentage}  
      then # percentInfectedAfterSaturation({s.rval(11)}, {10.0})  
      else # percentInfectedAfterSaturation({percentage}, {count - 1.0})  
    fi fi;  
eval E[percentInfectedAfterSaturation({0.0}, {10.0})];
```

В данном примере мы инициируем расчет командой eval, вызывая рекурсивную по времени функцию percentInfectedAfterSaturation, в которой изначальный процент инфицированных хостов положен равным 0, а время до насыщения – 10 временным интервалам. Система рассчитывает математическое ожидание, дисперсию и доверительный интервал. В результате имеем, что процент зараженных узлов при достижении полного насыщения лежит в доверительном интервале [0,15; 0,2].

Максимальная скорость распространения вируса. Получим оценку значения метрики 2 с помощью следующего MultiQuaTEx-выражения:

```
MaxInfectionSpeed(speed, percentage, count) =  
  if {count <= 0.0} then {speed} else  
    if {s.rval(11) percentage > speed}  
      then # MaxInfectionSpeed ({s.rval(11) percentage}, {s.rval(11)}, {10.0})  
      else # MaxInfectionSpeed ({speed}, {percentage}, {count 1.0})  
    fi fi;  
eval E[MaxInfectionSpeed ({0.0}, {0.0}, {10.0})];
```

Здесь мы инициируем расчет командой eval, вызывая рекурсивную по времени функцию MaxInfectionSpeed, в которой изначальная скорость заражения и процент инфицированных хостов положены равными 0, а время до насыщения – 10 временным шагам. В итоге имеем, что максимальная скорость заражения узлов лежит в доверительном интервале [0,07; 0,11].

Время до объявления насыщения вируса. Для вычисления оценки значения метрики 3 используем следующее MultiQuaTEx-выражение:

```
SaturationTime(percentage, count) =  
  if {count <= 0.0} then {s.rval(1)} else  
    if {s.rval(11) > percentage}  
      then # SaturationTime({s.rval(11)}, {10.0})  
      else # SaturationTime({percentage}, {count - 1.0})  
    fi fi;  
eval E[SaturationTime({0.0}, {10.0})];
```

В данном случае мы инициируем расчет командой eval, вызывая рекурсивную по времени функцию SaturationTime, где процент инфицированных хостов в начальный момент времени положен равным 0, а время до насыщения – 10 временным шагам. Полученное время до насыщения лежит в доверительном интервале [13,3; 13,9].

Анализ результатов статистического анализа

Важность обновления групп оповещений отдельных узлов продемонстрирована в [14], где были найдены контркарantinные стратегии вирусного распространения, использующие факт статической структуры групп. Для изучения значения алгоритма выбора групп мы исследовали модификацию алгоритма защиты с «неудачным» алгоритмом выбора групп, не обеспечивающим равномерное покрытие узлов группами в силу того, что каждый узел выбирает членов своей группы случайным образом не из всего множества узлов, а лишь из узлов, идентификаторы id которых расположены близко от него. Таким образом, некоторые узлы не получают достаточного количества оповещений, чтобы вовремя перейти в режим защиты.

После изменения алгоритма выбора членов групп мы повторили статистический анализ метрик 1–3 и получили следующие результаты:

- эффективность системы защиты понизилась, о чем свидетельствует распространение вируса с течением времени (рис. 2);
- процент зараженных хостов по достижении насыщения стал оцениваться доверительным интервалом $[0,54; 0,63]$ вместо ранее полученного $[0,15; 0,20]$;
- максимальная скорость заражения узлов оказалась в интервале $[0,16; 0,21]$ вместо ранее оцененного $[0,07; 0,11]$;
- время до насыщения оказалось в интервале $[24,6; 27,2]$ вместо ранее оцененного $[13,3; 13,9]$.

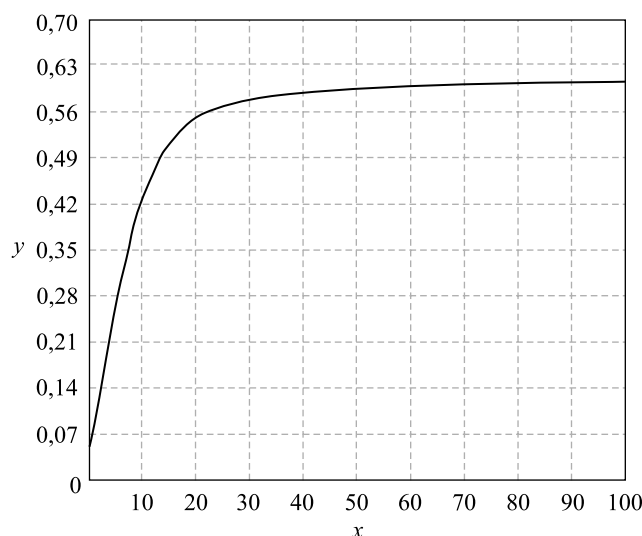


Рис. 2. Распространение вируса в случае неравномерного покрытия узлов группами оповещения

Fig. 2. Virus propagation in case of uneven coverage of nodes by alert groups

Из результатов видно, что «дефект» системы оказывает существенное влияние на ее эффективность и наглядно демонстрирует, как статистическая верификация помогает обнаружить неявные проблемы дизайна систем защиты. Данный «дефект» вполне может быть выявлен на этапе проектирования системы, и на этом этапе можно произвести ее доработку до последующего аналитического исследования, что иллюстрирует преимущество излагаемого подхода к разработке подобных систем.

Мы также изучили возможность «упрощения» системы путем исключения алгоритмического шага формирования групп. В данной модификации алгоритма узлы оповещают случайно выбранные узлы из всего множества узлов. Для такой модификации мы не обнаружили ухудшения эффективности системы защиты при выбранных параметрах. Поэтому при последующих исследованиях необходимо обратить внимание на указанное сокращение алгоритма, которое также иллюстрирует возможность потенциальных существенных «упрощений» системы на ранних этапах ее разработки.

Заключение

В статье проиллюстрирован подход к разработке модели сложных динамических распределенных стохастических систем с коммуникацией на ранних этапах, до проведения ее аналитического анализа, на примере предварительной модели стохастической групповой системы защиты от вирусов и экспериментов с ней. Данный подход базируется на модели РООСГС [1] и статистическом анализе, описанном в [2]. Продemonстрировано, как получение оценки основных численных параметров системы, обычно используемых для оценки систем подобного типа, дает возможность оценить систему до фиксации формальной модели и проведения полноценного анализа. В условиях предварительного эксперимента установлено, что система защиты позволяет сохранить значительный процент узлов незараженными при атаке вируса со случайным выбором заражаемого узла.

Изучено влияние алгоритма выбора групп оповещения на эффективность системы защиты. Анализ показывает, что важным условием этой эффективности является равномерное покрытие всего множества узлов группами оповещения, что обуславливает необходимость более тщательного изучения данного факта впоследствии. В нашем эксперименте также обнаружено, что существенное «упрощение»

алгоритма выбора групп оповещения не повлияло на эффективность системы. Это указывает на потенциальную возможность такого «упрощения» с сохранением свойств системы, что может быть проверено на более поздних этапах разработки. Можно утверждать, что применение изложенного статистического исследования систем на этапе их проектирования позволяет изучить важные аспекты системы до ее анализа аналитическими методами и на этом этапе исправить «дефекты» и определить некоторые потенциальные «упрощения» отдельных компонент, что может дать преимущество на более поздних стадиях разработки.

Библиографические ссылки

1. Шарыкин РЕ, Курбачкий АН. Модель распределенных объектно ориентированных стохастических гибридных систем. *Журнал Белорусского государственного университета. Математика. Информатика*. 2019;2:52–61. DOI: 10.33581/2520-6508-2019-2-52-61.
2. Шарыкин РЕ, Курбачкий АН. Верификация распределенных объектно ориентированных стохастических гибридных систем. *Вестник Гродненского государственного университета имени Янки Купалы. Серия 2. Математика. Физика. Информатика, вычислительная техника и управление*. 2019;9(3):123–132.
3. Meseguer J. Conditional rewriting logic as a unified model of concurrency. *Theoretical Computer Science*. 1992;96(1):73–155. DOI: 10.1016/0304-3975(92)90182-F.
4. Martí-Oliet N, Meseguer J. Rewriting logic: roadmap and bibliography. *Theoretical Computer Science*. 2002;285(2):121–154. DOI: 10.1016/S0304-3975(01)00357-7.
5. Clavel M, Durán F, Eker S, Lincoln P, Martí-Oliet N, Meseguer J, et al. Maude: Specification and programming in rewriting logic. *Theoretical Computer Science*. 2002;285(2):187–243. DOI: 10.1016/S0304-3975(01)00359-0.
6. Clavel M, Durán F, Eker S, Meseguer J. Chapter 1. Building equational proving tools by reflection in rewriting logic. In: Futatsugi K, Nakagawa AT, Tamai T, editors. *CAFE: an industrial-strength algebraic formal method*. [S. l.]: Elsevier; 2000. p. 1–31. DOI: 10.1016/B978-044450556-9/50061-7.
7. Sen K, Viswanathan M, Agha G. On statistical model checking of stochastic systems. In: Etesami K, Rajamani SK, editors. *Computer aided verification. Proceedings of the 17th International conference on computer aided verification*. Berlin: Springer; 2005. p. 266–280. (Lecture notes in computer science; volume 3576). DOI: 10.1007/11513988_26.
8. Briesmeister L, Porras P. Microscopic simulation of a group defense strategy. In: Nicol D, editor. *Proceedings of the 19th Workshop on principles of advanced and distributed simulation; 2005 June 1–3; Monterey, USA*. Los Alamitos: IEEE Computer Society; 2005. p. 254–261. DOI: 10.1109/PADS.2005.13.
9. Anagnostakis KG, Greenwald MB, Ioannidis S, Keromytis AD, Li D. A cooperative immunization system for untrusting Internet. In: Moreton N, editor. *The 11th IEEE International conference on networks; 2003 September 28 – October 1; Sydney, Australia*. Los Alamitos: IEEE Computer Society; 2003. p. 403–408. DOI: 10.1109/ICON.2003.1266224.
10. Nojiri D, Rowe J, Levitt K. Cooperative response strategies for large scale attack mitigation. In: Werner B, editor. *Proceedings DARPA information survivability conference and exposition; 2003 April 22–24; Washington, USA*. Los Alamitos: IEEE Computer Society; 2003. p. 293–302. DOI: 10.1109/DISCEX.2003.1194893.
11. Twycross J, Williamson MM. Implementing and testing a virus throttle. In: Paxson V, editors. *Proceedings of the 12th conference on USENIX security symposium; 2003 August 4–8; Washington, USA*. Berkeley: USENIX Association; 2003. p. 285–294.
12. Singh S, Estan C, Varghese G, Savage S. Automated worm fingerprinting. In: Brewer E, editor. *Proceedings of the 6th conference on symposium on operating systems design and implementation; 2004 December 6–8; San Francisco, USA*. Berkeley: USENIX Association; 2004. p. 45–60.
13. Kim H-A, Karp B. Autograph: Toward automated, distributed worm signature detection. In: Blaze M, editor. *Proceedings of the 13th conference on USENIX security symposium; 2004 August 9–13; San Diego, USA*. Berkeley: USENIX, The Advanced Computing Systems Association; 2004. p. 271–286.
14. Briesmeister L, Porras P. Automatically deducing propagation sequences that circumvent a collaborative worm defense. In: Hasanein H, editor. *Proceedings of the International performance computing and communications conference; 2006 April 10–12; Phoenix, USA*. Los Alamitos: IEEE Computer Society; 2006. p. 587–592. DOI: 10.1109/2006.1629456.
15. Шарыкин РЕ. Спецификация коллаборационной системы защиты от вирусных атак в среде Maude [Интернет]. GitHub [протитировано 2 января 2020 г.]. Доступно по: <https://github.com/shymaude/virusDefense/blob/master/defense.shymaude>.
16. Briesmeister L, Porras PA, Tiwari A (Computer Science Laboratory). Model checking of worm quarantine and counter-quarantine under a group defense. Technical Report. Menlo Park: SRI International; 2005. Technical Report Number: SRI-CSL-05-03, SRI Project 13738.
17. Sebastio S, Vandin A. MultiVeStA: statistical model checking for discrete event simulators. In: Horvath A, editor. *Proceedings of the 7th International conference on performance evaluation methodologies and tools; 2013 December 10–12; Torino, Italy*. Brussels: Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering; 2013. p. 310–315. DOI: 10.4108/icst.valuetools.2013.254377.
18. AlTurki M, Meseguer J. PVeStA: a parallel statistical model checking and quantitative analysis tool. In: Corradini A, Klin B, Cirstea C, editors. *Algebra and coalgebra in computer science. International conference on algebra and coalgebra in computer science*. Berlin: Springer; 2011. p. 386–392. (Lecture notes in computer science; volume 6859).

References

1. Sharykin RE, Kourbatski AN. A model of distributed object-based stochastic hybrid systems. *Journal of the Belarusian State University. Mathematics and Informatics*. 2019;2:52–61. Russian. DOI: 10.33581/2520-6508-2019-2-52-61.
2. Sharykin RE, Kourbatski AN. Verification of distributed object-oriented stochastic hybrid systems. *Vestnik Grodenskogo gosudarstvennogo universiteta imeni Yanki Kupaly. Seriya 2. Matematika. Fizika. Informatika, vychislitel'naya tekhnika i upravlenie*. 2019;9(3):123–132. Russian.

3. Meseguer J. Conditional rewriting logic as a unified model of concurrency. *Theoretical Computer Science*. 1992;96(1):73–155. DOI: 10.1016/0304-3975(92)90182-F.
4. Martí-Oliet N, Meseguer J. Rewriting logic: roadmap and bibliography. *Theoretical Computer Science*. 2002;285(2):121–154. DOI: 10.1016/S0304-3975(01)00357-7.
5. Clavel M, Durán F, Eker S, Lincoln P, Martí-Oliet N, Meseguer J, et al. Maude: Specification and programming in rewriting logic. *Theoretical Computer Science*. 2002;285(2):187–243. DOI: 10.1016/S0304-3975(01)00359-0.
6. Clavel M, Durán F, Eker S, Meseguer J. Chapter 1. Building equational proving tools by reflection in rewriting logic. In: Futatsugi K, Nakagawa AT, Tamai T, editors. *CAFE: an industrial-strength algebraic formal method*. [S. l.]: Elsevier; 2000. p. 1–31. DOI: 10.1016/B978-044450556-9/50061-7.
7. Sen K, Viswanathan M, Agha G. On statistical model checking of stochastic systems. In: Etessami K, Rajamani SK, editors. *Computer aided verification. Proceedings of the 17th International conference on computer aided verification*. Berlin: Springer; 2005. p. 266–280. (Lecture notes in computer science; volume 3576). DOI: 10.1007/11513988_26.
8. Briesmeister L, Porras P. Microscopic simulation of a group defense strategy. In: Nicol D, editor. *Proceedings of the 19th Workshop on principles of advanced and distributed simulation; 2005 June 1–3; Monterey, USA*. Los Alamitos: IEEE Computer Society; 2005. p. 254–261. DOI: 10.1109/PADS.2005.13.
9. Anagnostakis KG, Greenwald MB, Ioannidis S, Keromytis AD, Li D. A cooperative immunization system for untrusting Internet. In: Moreton N, editor. *The 11th IEEE International conference on networks; 2003 September 28 – October 1; Sydney, Australia*. Los Alamitos: IEEE Computer Society; 2003. p. 403–408. DOI: 10.1109/ICON.2003.1266224.
10. Nojiri D, Rowe J, Levitt K. Cooperative response strategies for large scale attack mitigation. In: Werner B, editor. *Proceedings DARPA information survivability conference and exposition; 2003 April 22–24; Washington, USA*. Los Alamitos: IEEE Computer Society; 2003. p. 293–302. DOI: 10.1109/DISCEX.2003.1194893.
11. Twycross J, Williamson MM. Implementing and testing a virus throttle. In: Paxson V, editors. *Proceedings of the 12th conference on USENIX security symposium; 2003 August 4–8; Washington, USA*. Berkeley: USENIX Association; 2003. p. 285–294.
12. Singh S, Estan C, Varghese G, Savage S. Automated worm fingerprinting. In: Brewer E, editor. *Proceedings of the 6th conference on symposium on operating systems design and implementation; 2004 December 6–8; San Francisco, USA*. Berkeley: USENIX Association; 2004. p. 45–60.
13. Kim H-A, Karp B. Autograph: Toward automated, distributed worm signature detection. In: Blaze M, editor. *Proceedings of the 13th conference on USENIX security symposium; 2004 August 9–13; San Diego, USA*. Berkeley: USENIX, The Advanced Computing Systems Association; 2004. p. 271–286.
14. Briesmeister L, Porras P. Automatically deducing propagation sequences that circumvent a collaborative worm defense. In: Hasanein H, editor. *Proceedings of the International performance computing and communications conference; 2006 April 10–12; Phoenix, USA*. Los Alamitos: IEEE Computer Society; 2006. p. 587–592. DOI: 10.1109/2006.1629456.
15. Sharykin RE. Maude specification of the stochastic collaborative virus defense system [Internet]. GitHub [cited 2020 January 2]. Available from: <https://github.com/shymaude/virusDefense/blob/master/defense.shymaude>.
16. Briesemeister L, Porras PA, Tiwari A (Computer Science Laboratory). Model checking of worm quarantine and counter-quarantine under a group defense. Technical Report. Menlo Park: SRI International; 2005. Technical Report Number: SRI-CSL-05-03, SRI Project 13738.
17. Sebastio S, Vandin A. MultiVeStA: statistical model checking for discrete event simulators. In: Horvath A, editor. *Proceedings of the 7th International conference on performance evaluation methodologies and tools; 2013 December 10–12; Torino, Italy*. Brussels: Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering; 2013. p. 310–315. DOI: 10.4108/icst.valuetools.2013.254377.
18. AlTurki M, Meseguer J. PVeStA: a parallel statistical model checking and quantitative analysis tool. In: Corradini A, Klin B, Cirstea C, editors. *Algebra and coalgebra in computer science. International conference on algebra and coalgebra in computer science*. Berlin: Springer; 2011. p. 386–392. (Lecture notes in computer science; volume 6859).

УДК 519.213

НОВЫЕ ВЕРХНИЕ ГРАНИЦЫ ДЛЯ ФУНКЦИИ НЕЦЕНТРАЛЬНОГО ХИ-КВАДРАТ РАСПРЕДЕЛЕНИЯ

В. А. ВОЛОШКО¹⁾, Е. В. ВЕЧЕРКО¹⁾

¹⁾Научно-исследовательский институт прикладных проблем математики и информатики БГУ,
пр. Независимости, 4, 220030, г. Минск, Беларусь

Некоторые новые верхние границы для функции нецентрального хи-квадрат распределения выводятся из базовых симметрий плотности многомерного стандартного нормального закона: унитарной инвариантности, независимости компонент как в полярной, так и в декартовой системе координат. В сравнении с известными в литературе аналогами предложенные новые верхние оценки имеют простой аналитический вид: они представляют собой комбинации из экспонент, прямых и обратных тригонометрических функций, в том числе гиперболических, а также функции распределения одномерного стандартного нормального закона. Данные оценки могут быть полезны как в теории, так и в приложениях для доказательства неравенств, связанных с функцией нецентрального хи-квадрат распределения, и построения нижних оценок мощности хи-квадрат критерия Пирсона.

Ключевые слова: нецентральное хи-квадрат распределение; верхняя граница.

Образец цитирования:

Волошко ВА, Вечерко ЕВ. Новые верхние границы для функции нецентрального хи-квадрат распределения. *Журнал Белорусского государственного университета. Математика. Информатика*. 2020;1:70–74 (на англ.).
<https://doi.org/10.33581/2520-6508-2020-1-70-74>

For citation:

Voloshko VA, Vecherko EV. New upper bounds for noncentral chi-square cdf. *Journal of the Belarusian State University. Mathematics and Informatics*. 2020;1:70–74.
<https://doi.org/10.33581/2520-6508-2020-1-70-74>

Авторы:

Валерий Анатольевич Волошко – кандидат физико-математических наук; старший научный сотрудник лаборатории математических методов защиты информации.
Егор Валентинович Вечерко – кандидат физико-математических наук, доцент; заведующий лабораторией математических методов защиты информации.

Authors:

Valeriy A. Voloshko, PhD (physics and mathematics); senior researcher at the laboratory of mathematical methods of information security.
valeravoloshko@yandex.ru
<https://orcid.org/0000-0002-9693-0688>
Egor V. Vecherko, PhD (physics and mathematics), docent; head of the laboratory of mathematical methods of information security.
vecherko@bsu.by

NEW UPPER BOUNDS FOR NONCENTRAL CHI-SQUARE CDF

V. A. VOLOSHKO^a, E. V. VECHERKO^a

^aResearch Institute for Applied Problems of Mathematics and Informatics,
Belarusian State University, 4 Niezaliežnasci Avenue, Minsk 220030, Belarus

Corresponding author: V. A. Voloshko (valeravoloshko@yandex.ru)

Some new upper bounds for noncentral chi-square cumulative density function are derived from the basic symmetries of the multidimensional standard Gaussian distribution: unitary invariance, components independence in both polar and Cartesian coordinate systems. The proposed new bounds have analytically simple form compared to analogues available in the literature: they are based on combination of exponents, direct and inverse trigonometric functions, including hyperbolic ones, and the cdf of the one dimensional standard Gaussian law. These new bounds may be useful both in theory and in applications: for proving inequalities related to noncentral chi-square cumulative density function, and for bounding powers of Pearson's chi-squared tests.

Keywords: noncentral chi-square distribution; upper bound.

Introduction

Let $d \in \mathbb{N}$, $\mu = (\mu_i)_{i=1}^d \in \mathbb{R}^d$, $\lambda = \|\mu\|^2 = \sum_{i=1}^d \mu_i^2$. Then the cumulative distribution function (cdf) of the non-central chi-square distribution with d degrees of freedom and noncentrality parameter λ is defined as follows:

$$f(x, d, \lambda) = \text{prob}\{\|\xi - \mu\|^2 \leq x\}, \quad x \geq 0. \quad (1)$$

Here $\xi \in \mathbb{R}^d$ is a standard normally distributed random d -vector. For the central chi-square cdf ($\lambda = 0$) we use brief notation $f(x, d) := f(x, d, 0)$.

The function (1) plays an important role in mathematical statistics. In particular, consider the classical problem of statistical hypothesis testing of null-hypothesis $H_0: L\{y_i\} = p = (p_i)_{i=1}^K$ (T observed i. i. d. random variables $\{y_i\}_{i=1}^T$, $y_i \in \{1, \dots, K\}$, have their common mass probability function $p_i: \{1, \dots, K\} \rightarrow \mathbb{R}_+$) against point alternative hypothesis $H_1: L\{y_i\} = q = (q_i)_{i=1}^K$. If the significance level $\alpha \in (0, 1)$ is fixed, and H_1 is contiguous to H_0 , i. e. the following convergence holds:

$$T \sum_{i=1}^K \frac{(p_i - q_i)^2}{p_i} \rightarrow \lambda > 0$$

as $T \rightarrow \infty$, then the probability β of type 2 error of the standard Pearson's chi-squared test converges to $f(x, d, \lambda)$ with $d = K - 1$ and $x = F_{\chi_d^2}^{-1}(1 - \alpha)$ (quantile function for the central chi-square distribution with d degrees of freedom). Hence the upper bounds for (1) provide the lower bounds for asymptotic power of chi-squared test under contiguous alternatives.

The function (1) is well studied analytically, being closely related to the generalized Marcum functions [1; 2] and modified Bessel function of the first kind [3]. Various upper and lower bounds for (1) are also available in the literature [1; 4]. Analytical expressions for these bounds, however, are as complex as the ones for $f(x, d, \lambda)$, being based on transcendental functions like modified Bessel function [1] or the moments of truncated normal distribution [4]. We present here some new upper bounds for (1). These bounds are of a relatively simple analytical form and may be useful both in theory (proving inequalities related to (1)) and in applications (bounding powers of chi-squared tests).

Upper bounds for noncentral chi-square cdf

Since the value (1) equals a standard Gaussian measure of a ball $B_{\mu, \sqrt{x}}$ of radius $\sqrt{x}$ with center μ , our idea is to construct upper bounds of the form

$$f(x, d, \lambda) \leq \text{prob}\{\xi \in A\}, \quad B_{\mu, \sqrt{x}} \subset A \subset \mathbb{R}^d. \quad (2)$$

Let $\Pi_1, \Pi_2 \subset \mathbb{R}^d$ be orthogonally complemented subspaces. Minkowski sums $A_i = B_{\mu, \sqrt{x}} + \Pi_i$ are cylindrical sets containing $B_{\mu, \sqrt{x}}$. Due to properties of standard normal distribution, the events $\xi \in A_i$ are independent and $\text{prob}\{\xi \in A_i\} = f(x, d_i, \lambda_i)$, where $d_i = \dim \Pi_i$ and λ_i is a squared norm of an orthogonal projection of μ onto Π_i , $i = 1, 2$. The set $A = A_1 \cap A_2$ in (2) leads to the following upper bound.

Lemma 1. *Let $d = d_1 + d_2$, $\lambda = \lambda_1 + \lambda_2$, $\lambda_i \geq 0$, $d_i \in \mathbb{N}$, $i = 1, 2$. Then the following inequality holds:*

$$f(x, d, \lambda) \leq f(x, d_1, \lambda_1) f(x, d_2, \lambda_2). \quad (3)$$

Since $f(x, 1, \lambda) = \Phi\left|\frac{\sqrt{\lambda} + \sqrt{x}}{\sqrt{\lambda} - \sqrt{x}}\right|$, where $\Phi(\cdot)$ is the standard Gaussian cdf, we get from (3):

$$f(x, d, \lambda) \leq f(x, d-1, \lambda) \Phi\left|\frac{\sqrt{\lambda} + \sqrt{x}}{\sqrt{\lambda} - \sqrt{x}}\right|. \quad (4)$$

Repeated application of (3) also gives the following bounds:

$$f(x, d, \lambda) \leq \left(\Phi\left|\frac{\sqrt{\lambda/d} + \sqrt{x}}{\sqrt{\lambda/d} - \sqrt{x}}\right|\right)^d, \quad (5)$$

$$f(x, d, \lambda) \leq \left(\Phi\left|\frac{\sqrt{x}}{\sqrt{\lambda} - \sqrt{x}}\right|\right)^{d-1} \Phi\left|\frac{\sqrt{\lambda} + \sqrt{x}}{\sqrt{\lambda} - \sqrt{x}}\right|. \quad (6)$$

Another way to construct covering set A in (2) is based on unitary invariance of standard normal distribution. Namely, let us assume $d \geq 2$, $x \leq \lambda$, and define

$$A_1 = \{w \in \mathbb{R}^d : \|\|w\| - \sqrt{\lambda}\| \leq x\}, \quad A_2 = \{cw : c \geq 0, w \in B_{\mu, \sqrt{x}}\}.$$

According to mentioned unitary invariance, the events $\xi \in A_i$ are independent as well. It is easy to see that $\text{prob}\{\xi \in A_1\} = f(\cdot, d)\left|\frac{\sqrt{\lambda} + \sqrt{x}}{\sqrt{\lambda} - \sqrt{x}}\right|^2$, while A_2 is a cone and $\text{prob}\{\xi \in A_2\}$ equals normalized Lebesgue measure of a spherical ball $A_2 \cap S^{d-1}$ of radius $\arcsin \sqrt{\frac{x}{\lambda}}$ (in spherical metric, S^{d-1} is the unit sphere in $\mathbb{R}^d$). Hence we get the following lemma.

Lemma 2. *The following inequality holds for $d \geq 2$, $x \leq \lambda$:*

$$f(x, d, \lambda) \leq f(\cdot, d)\left|\frac{\sqrt{\lambda} + \sqrt{x}}{\sqrt{\lambda} - \sqrt{x}}\right|^2 \frac{\Gamma\left(\frac{d}{2}\right)}{\Gamma\left(\frac{d-1}{2}\right)\sqrt{\pi}} \int_0^{\arcsin \sqrt{\frac{x}{\lambda}}} (\sin \rho)^{d-2} d\rho, \quad (7)$$

where $\Gamma(\cdot)$ is Gamma function.

Using the inequalities $\text{prob}\{\xi \in A_2\} \leq \frac{1}{2}$, $\frac{\Gamma\left(z + \frac{1}{2}\right)}{\Gamma(z)} \leq \sqrt{z}$, $z > 0$, and

$$\int_0^{\rho_*} (\sin \rho)^{d-2} d\rho \leq \int_0^{\rho_*} (\sin \rho)^{d-2} \frac{d \sin \rho}{\cos \rho_*} = \frac{(\sin \rho_*)^{d-1}}{(d-1) \cos \rho_*}, \quad \forall \rho_* \in \left(0, \frac{\pi}{2}\right),$$

we obtain a weakened version of (7) having more explicit form:

$$f(x, d, \lambda) \leq f(\cdot, d)\left|\frac{\sqrt{\lambda} + \sqrt{x}}{\sqrt{\lambda} - \sqrt{x}}\right|^2 \min \left\{ \frac{1}{2}, \sqrt{\frac{\left(\frac{x}{\lambda}\right)^{d-1}}{2\pi(d-1)\left(1 - \frac{x}{\lambda}\right)}} \right\}, \quad d \geq 2, x \leq \lambda. \quad (8)$$

For even d the bound (7) has completely explicit form since central chi-square pdf is integrable.

Corollary. *The following inequalities hold for $x \leq \lambda$:*

$$f(x, 2, \lambda) \leq \frac{2}{\pi} e^{-\frac{1}{2}(\lambda+x)} \sinh \sqrt{\lambda x} \arcsin \sqrt{\frac{x}{\lambda}}, \quad (9)$$

$$f(x, 4, \lambda) \leq \frac{2}{\pi} e^{-\frac{1}{2}(\lambda+x)} \left(\left(1 + \frac{\lambda+x}{2} \right) \sinh \sqrt{\lambda x} - \sqrt{\lambda x} \cosh \sqrt{\lambda x} \right) \times \\ \times \left(\arcsin \sqrt{\frac{x}{\lambda}} - \lambda^{-1} \sqrt{x(\lambda-x)} \right). \quad (10)$$

Combining (3) with (9), we get the following bounds for even $d = 2k$ and $x \leq \frac{\lambda}{k}$:

$$f(x, 2k, \lambda) \leq e^{-\frac{1}{2}(\lambda+kx)} \left(\frac{2}{\pi} \sinh \sqrt{\frac{\lambda x}{k}} \arcsin \sqrt{\frac{kx}{\lambda}} \right)^k, \quad (11)$$

$$f(x, 2k, \lambda) \leq \frac{2}{\pi} e^{-\frac{1}{2}(\lambda+kx)} \sinh^{k-1}(x) \sinh \sqrt{\lambda_* x} \arcsin \sqrt{\frac{x}{\lambda_*}}, \quad (12)$$

where $\lambda_* = \lambda - (k-1)x$. The bounds similar to (11), (12) can be obtained from (10) for $d = 4k$.

Computer experiments

The four plots on the fig. 1 illustrate the upper bounds for (1) proposed in the paper. On the plots on fig. 1, a, b, d , we see that the corresponding upper bounds are strictly ordered for the chosen d and λ . This observation allows us to formulate the conjecture that the upper bounds for (1) are ordered as follows: «(6) $\leq$ (5)» for any $x \geq 0$, $d \in \mathbb{N}$, $\lambda \geq 0$; «(11) $\leq$ (12)» for any $0 \leq x \leq \frac{\lambda}{k}$, $d = 2k$ (even), $\lambda \geq 0$; «(10) $\leq$ (6) $\leq$ (11)» for any $0 \leq x \leq \frac{\lambda}{2}$, $d = 4$, $\lambda \geq 0$. The inequality «(4) $\leq$ (6)» is not listed, because it obviously follows from (5). The plot fig. 1, c , allows to conjecture that for $d \geq 2$ the upper bound (8) is better than (4) for small $x \leq x_*$ up to some $x_* \leq \lambda_*$, and vice versa for $x_* \leq x \leq \lambda_*$.

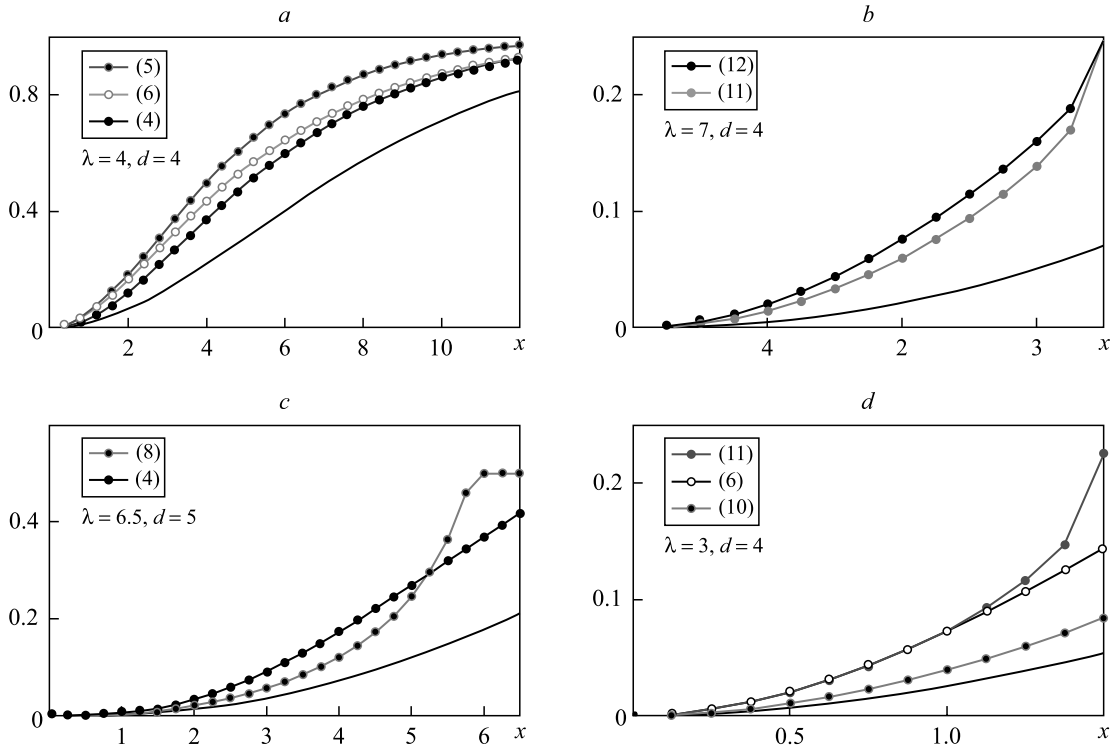


Fig. 1. Noncentral chi-square cdf (1) (lower black lines) and its upper bounds (upperbroken lines)

The plot on the fig. 2 illustrates dependence of the type 2 error β of chi-square test on data volume T under alternative H_1 contiguous to H_0 :

$$T \sum_{i=1}^K \frac{(p_i - q_i)^2}{p_i} \rightarrow \lambda = 7,$$

where $K = 5$; $p = (p_i) = (0.05, 0.1, 0.15, 0.3, 0.4)$. The threshold of chi-square test $x = 6$ corresponds to the significance level $\alpha = 1 - F_{\chi_{K-1}^2}(x) \approx 0.2$. The upper level $\beta_{\max} \approx 0.265$ on the plot corresponds to the upper bound (10) for $x = 6$, $\lambda = 7$.

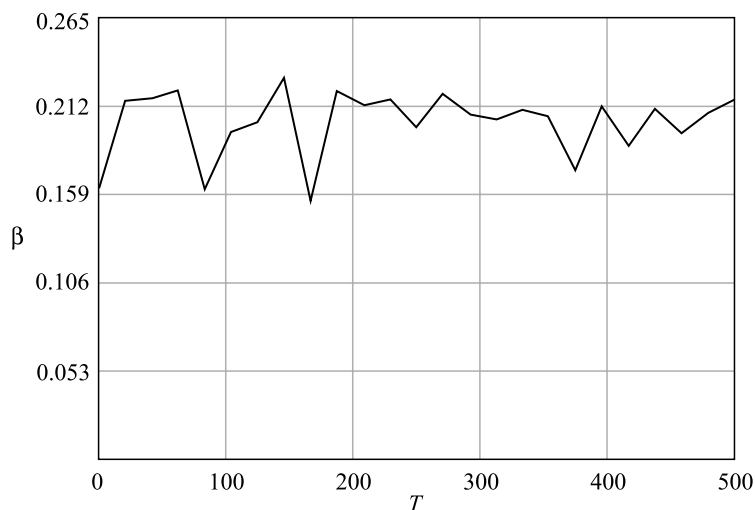


Fig. 2. Chi-square test type 2 error β against data volume T

References

1. Segura J. Monotonicity properties and bounds for the chi-square and gamma distributions. *Applied Mathematics and Computation*. 2014;246:399–415. DOI: 10.1016/j.amc.2014.08.034.
2. Andras Sz, Baricz A, Sun Y. The generalized marcum Q -function: an orthogonal polynomial approach. *Acta Universitatis Sapientiae. Mathematica*. 2011;3(1):60–76.
3. Bateman H, Erdelyi A. *Higher transcendental functions. Volume 2*. New York: McGraw-Hill; 1953. XVIII + 396 p.
4. Cook JD. Upper bounds on non-central chi-squared tails and truncated normal moments. *UT MD Anderson Cancer Center Department of Biostatistics Working Paper Series* [Internet]. 2010 [cited 2020 January 11];62. Available from: https://www.johndcook.com/non_central_chi_square.pdf.

Received by editorial board 19.02.2020.

ОПТИМИЗАЦИЯ ЛИНЕЙНОЙ ДИНАМИЧЕСКОЙ СИСТЕМЫ С ПЕРИОДИЧЕСКИМИ БЫСТРОМЕНЯЮЩИМИСЯ КОЭФФИЦИЕНТАМИ

В. В. КРАХОТКО¹⁾, Г. П. РАЗМЫСЛОВИЧ¹⁾, В. В. ГОРЯЧКИН¹⁾

¹⁾Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь

Рассматривается задача оптимального управления линейной динамической системы с периодическими параметрами. Качественная теория таких задач разработана весьма полно, если период коэффициентов системы не очень мал. В случае малого периода возникают серьезные трудности с интегрированием, поэтому разумно дополнить конструктивные методы решения асимптотическими. Для решения поставленной задачи строится вспомогательная (базовая) задача, при исследовании которой применяется метод усреднения. Получены оценки близости решений исходной и базовой задач.

Ключевые слова: линейные системы; оптимальное управление; системы с малым параметром; асимптотические методы.

OPTIMIZATION OF A LINEAR DYNAMIC SYSTEM WITH PERIODIC CHANGING PARAMETERS

V. V. KRAKHOTKO^a, G. P. RAZMYSLOVICH^a, V. V. GORYACHKIN^a

^aBelarusian State University, 4 Niezaliežnasci Avenue, Minsk 220030, Belarus

Corresponding author: G. P. Razmyslovich (razmysl@bsu.by)

The article deals with the problem of optimal control of a linear dynamic system with periodic parameters. The qualitative theory of such problems is developed very fully if the period of coefficients of the system is not very small. With a small period, there are serious difficulties with integration. Therefore, it is reasonable to supplement the constructive methods of solution with asymptotic ones. The article presents such an approach that the method of averaging is used to construct an auxiliary (basic) problem, estimates of the proximity of solutions to the initial and basic problems are obtained.

Keywords: linear systems; optimal control; systems with small parameters; asymptotic methods.

Образец цитирования:

Крахотко ВВ, Размыслович ГП, Горячкин ВВ. Оптимизация линейной динамической системы с периодическими быстроменяющимися коэффициентами. *Журнал Белорусского государственного университета. Математика. Информатика*. 2020;1:75–79.
<https://doi.org/10.33581/2520-6508-2020-1-75-79>

For citation:

Krakhotko VV, Razmyslovich GP, Goryachkin VV. Optimization of a linear dynamic system with periodic changing parameters. *Journal of the Belarusian State University. Mathematics and Informatics*. 2020;1:75–79. Russian.
<https://doi.org/10.33581/2520-6508-2020-1-75-79>

Авторы:

Валерий Васильевич Крахотко – кандидат физико-математических наук, доцент; доцент кафедры оптимального управления факультета прикладной математики и информатики.

Георгий Прокофьевич Размыслович – кандидат физико-математических наук, доцент; доцент кафедры высшей математики факультета прикладной математики и информатики.

Владимир Владимирович Горячкин – кандидат физико-математических наук, доцент; доцент кафедры технологии программирования факультета прикладной математики и информатики.

Authors:

Valerii V. Krakhotko, PhD (physics and mathematics), docent; associate professor at the department of optimal control, faculty of applied mathematics and computer science.
krakhotko@bsu.by

Georgii P. Razmyslovich, PhD (physics and mathematics), docent; associate professor at the department of higher mathematics, faculty of applied mathematics and computer science.
razmysl@bsu.by

Vladimir V. Goryachkin, PhD (physics and mathematics), docent; associate professor at the department of programming technologies, faculty of applied mathematics and computer science.
goryachkin@bsu.by

Рассмотрим задачу оптимального управления линейной нестационарной системы

$$J(u) = c'x(t_1^*) \rightarrow \max, \quad (1)$$

$$\dot{x}(t) = A_\mu(t)x(t) + bu(t), \quad x(t_0) = x_0, \quad Hx(t_1^*) = q, \quad |u(t)| \leq 1, \quad t \in T = [t_0, t_1^*],$$

где $x \in \mathbb{R}^n$, $u \in \mathbb{R}$, $H \in \mathbb{R}_{m,n}$, $b, c \in \mathbb{R}^n$, $q \in \mathbb{R}^m$; $A_\mu(\cdot)$ – семейство μ -периодических [1; 2] измеримых матриц-функций размера $n \times n$, $\mu > 0$, причем $\exists \mu_0 > 0$ такое, что $\forall \mu \in (0, \mu_0]$ $\max_{t \in T} \|A_\mu(t)\| \leq L$; x_0 – заданный n -вектор.

Управление $u(t)$ будем называть допустимым, если оно является кусочно-непрерывной функцией на отрезке T .

Введем в рассмотрение матрицу $A_\mu = \frac{1}{\mu} \int_{t_0}^{t_0 + \mu} A_\mu(t) dt$. Будем также считать, что существует $n \times n$ -матрица A такая, что $A = \lim_{\mu \rightarrow 0} A_\mu$.

Наряду с задачей (1) рассмотрим усредненную задачу [3]

$$J_1(u) = c'x^*(t_1^*) \rightarrow \max, \quad (2)$$

$$\dot{x}^*(t) = Ax^*(t) + bu(t), \quad x^*(t_0) = x_0, \quad Hx^*(t_1^*) = q, \quad |u(t)| \leq 1, \quad t \in T.$$

Пусть $x(t, u)$ и $x^*(t, u)$ – решения систем $\dot{x} = A_\mu(t)x + bu$ и $\dot{x}^* = Ax^* + bu$ соответственно при одном и том же управлении $u(t)$.

Оценим норму разности этих решений, а именно $\|x(t, u) - x^*(t, u)\|$. В силу (1), (2) имеем

$$\|x(t, u) - x^*(t, u)\| = \left\| \int_{t_0}^t A_\mu(\tau) (x(\tau, u) - x^*(\tau, u)) d\tau + \right.$$

$$\left. + \int_{t_0}^t (A_\mu(\tau) - A) \left(e^{A(\tau-t_0)} x_0 + \int_{t_0}^{\tau} e^{A(\tau-s)} bu(s) ds \right) d\tau \right\| = \|J_1 + J_2 + J_3\|, \quad (3)$$

где $J_1 = \int_{t_0}^t A_\mu(\tau) (x(\tau, u) - x^*(\tau, u)) d\tau$; $J_2 = \int_{t_0}^t (A_\mu(\tau) - A_\mu) \left(e^{A(\tau-t_0)} x_0 + \int_{t_0}^{\tau} e^{A(\tau-s)} bu(s) ds \right) d\tau$; $J_3 = \int_{t_0}^t (A_\mu - A) \left(e^{A(\tau-t_0)} x_0 + \int_{t_0}^{\tau} e^{A(\tau-s)} bu(s) ds \right) d\tau$.

Рассмотрим в (3) интеграл J_2 на отрезке T и оценим его. Положим $m = \left\lceil \frac{t_1^* - t_0}{\mu} \right\rceil$, $t_k = t_0 + k\mu$, $k = 0, 1, \dots, m$. Тогда

$$\int_{t_0}^{t_1^*} (A_\mu(\tau) - A_\mu) \left(e^{A(\tau-t_0)} x_0 + \int_{t_0}^{\tau} e^{A(\tau-s)} bu(s) ds \right) d\tau =$$

$$= \sum_{k=0}^{m-1} \int_{t_k}^{t_{k+1}} (A_\mu(\tau) - A_\mu) e^{A(t_k-t_0)} \left(E + \sum_{j=1}^{\infty} \frac{(t_k - t_k)^j}{j!} A^j \right) \left(x_0 + \int_{t_0}^{t_k} e^{-A(s-t_0)} bu(s) ds + \right.$$

$$\left. + \int_{t_k}^{\tau} e^{-A(s-t_0)} bu(s) ds \right) d\tau + \int_{t_{m-1}}^{t_1^*} (A_\mu(\tau) - A_\mu) \left(e^{A(\tau-t_0)} x_0 + \int_{t_0}^{\tau} e^{A(\tau-s)} bu(s) ds \right) d\tau. \quad (4)$$

В силу определения матриц A_μ и A имеем $\|A_\mu(\tau) - A_\mu\| \leq 2L$, где матричная норма согласована с рассматриваемой векторной нормой. Следовательно,

$$\begin{aligned}
\|J_2\| &= \left\| \int_{t_0}^t (A_\mu(\tau) - A_\mu) \left(e^{A(\tau-t_0)} x_0 + \int_{t_0}^{\tau} e^{A(\tau-s)} bu(s) ds \right) d\tau \right\| \leq \left\| \int_{t_0}^{t_1^*} (A_\mu(\tau) - A_\mu) \left(e^{A(\tau-t_0)} x_0 + \right. \right. \\
&\quad \left. \left. + \int_{t_0}^{\tau} e^{A(\tau-s)} bu(s) ds \right) d\tau \right\| \leq \left\| \sum_{k=0}^{m-1} \int_{t_k}^{t_{k+1}} (A_\mu(\tau) - A_\mu) e^{A(t_k-t_0)} \left(E + \sum_{j=1}^{\infty} \frac{(\tau-t_k)^j}{j!} A^j \right) \times \right. \\
&\quad \times \left(x_0 + \int_{t_0}^{t_k} e^{-A(s-t_0)} bu(s) ds + \int_{t_k}^{\tau} e^{-A(s-t_0)} bu(s) ds \right) d\tau \left. \right\| + \left\| \int_{t_{m-1}}^{t_1^*} (A_\mu(\tau) - A_\mu) \left(e^{A(\tau-t_0)} x_0 + \right. \right. \\
&\quad \left. \left. + \int_{t_0}^{\tau} e^{-A(s-t_0)} bu(s) ds \right) d\tau \right\| \leq 2Le^{L(t_1^*-t_0)} (t_1^*-t_0) \mu (\|b\| + L(\|x_0\| + (t_1^*-t_0)\|b\|)) + \\
&\quad + 2Le^{L(t_1^*-t_0)} (\|x_0\| + (t_1^*-t_0)\|b\|) \mu = C_1 \mu,
\end{aligned}$$

где

$$C_1 = 2Le^{L(t_1^*-t_0)} (t_1^*-t_0) \|b\| + (L(t_1^*-t_0) + 1) (\|x_0\| + (t_1^*-t_0)\|b\|). \quad (5)$$

Далее интеграл J_3 в (3) на отрезке T оценивается следующим образом:

$$\begin{aligned}
\|J_3\| &= \left\| \int_{t_0}^{t_1^*} (A_\mu - A) \left(e^{A(\tau-t_0)} x_0 + \int_{t_0}^{\tau} e^{A(\tau-s)} bu(s) ds \right) d\tau \right\| \leq \\
&\leq e^{L(t_1^*-t_0)} (t_1^*-t_0) (\|x_0\| + (t_1^*-t_0)\|b\|) \|A_\mu - A\| = C_2 \|A_\mu - A\|,
\end{aligned} \quad (6)$$

где $C_2 = e^{L(t_1^*-t_0)} (t_1^*-t_0) (\|x_0\| + (t_1^*-t_0)\|b\|)$.

Итак, из (3) в силу (4)–(6) получим

$$\|x(t, u) - x^*(t, \mu)\| \leq L \int_{t_0}^t \|x(\tau, u) - x^*(\tau, u)\| d\tau + C(\mu + \|A_\mu - A\|), \text{ где } C = \max\{C_1, C_2\}.$$

Применяя к последнему неравенству лемму Гронуолла – Беллмана [4], имеем

$$\|x(t, u) - x^*(t, u)\| \leq C(\mu + \|A_\mu - A\|) e^{L(t_1^*-t_0)} = C_0(\mu + \|A_\mu - A\|), \quad (7)$$

где $C_0 = Ce^{L(t_1^*-t_0)}$.

Пусть $x^0(t) \equiv x(t, u^0)$, $u^0(t)$ – оптимальная траектория и оптимальное управление в задаче (1) соответственно, а $u^{*0}(t)$ – оптимальное управление в задаче (2), $t \in T$, $x(t, u^{*0})$ – траектория системы (1) при управлении $u^{*0}(t)$. Тогда

$$x^0(t) - x(t, u^{*0}) = \int_{t_0}^t A_\mu(\tau) (x^0(\tau) - x(\tau, u^{*0})) d\tau + \int_{t_0}^t b(u^0(\tau) - u^{*0}(\tau)) d\tau.$$

Отсюда следует, что

$$\|x^0(t) - x(t, u^{*0})\| \leq L \int_{t_0}^t \|x^0(\tau) - x(\tau, u^{*0})\| d\tau + \|b\| \int_{t_0}^t |u^0(\tau) - u^{*0}(\tau)| d\tau. \quad (8)$$

Согласно лемме Гронуолла – Беллмана из (8) получим

$$\|x^0(t) - x(t, u^{*0})\| \leq \|b\| e^{L(t_1^*-t_0)} \int_{t_0}^t |u^0(\tau) - u^{*0}(\tau)| d\tau. \quad (9)$$

Так как $u^0(t)$ и $u^{*0}(t)$ – оптимальные управления в задачах (1) и (2) соответственно, то согласно принципу максимума [5] имеем

$$u^0(t) = \text{sign } \psi'_\mu(t)b, \quad u^{*0}(t) = \text{sign } \psi'(t)b, \quad t \in T,$$

где $\psi_\mu(t)$ и $\psi(t)$ – решения сопряженных систем $\dot{\psi}_\mu = -A'_\mu(t)\psi_\mu$ и $\dot{\psi} = -A'\psi$ соответственно.

По аналогии с (7) имеет место оценка

$$\|\psi_\mu(t) - \psi(t)\| = o_\mu(1), \quad (10)$$

здесь $o_\mu(1)$ не зависит от $t, t \in T$.

Обозначим через $\tau_i, i = \overline{1, p}$, корни $\psi'(t)b$ на отрезке $[t_0, t_1^*]$, причем $t_0 \leq \tau_1 < \tau_2 < \dots < \tau_p \leq t_1^*$, а через k_i – их кратности. Пусть $\max_{i=\overline{1, p}} k_i = k, \min_{i=\overline{1, p}} |\psi^{(k_i)'}(\tau_i)b| = 2h$.

В силу непрерывности функций $\psi^{(k_i)'}(\tau)b, i = \overline{1, p}$, можно указать такое $l > 0$, что

$$|\psi^{(k_i)'}(\tau)b| > h, \quad \forall \tau \in [\tau_i - l, \tau_i + l], \quad i = \overline{1, p}. \quad (11)$$

Положим $d = \inf |\psi'(\tau)b|, \tau \notin [\tau_i - l, \tau_i + l], i = \overline{1, p}$. Тогда $|\psi'(\tau)b| > d, \forall \tau \notin [\tau_i - l, \tau_i + l], i = \overline{1, p}$.

В окрестности точек τ_i функция $\psi'_\mu(\tau)b$ представима в виде

$$\psi'_\mu(\tau)b = \psi'(\tau)b + (\psi'_\mu(\tau)b - \psi'(\tau)b) = \psi^{(k_i)'}(\tau)b \frac{(\tau - \tau_i)^{k_i}}{k_i!} + o_\mu(1), \quad (12)$$

где $\lim_{\mu \rightarrow 0} o_\mu(1) = 0$.

В силу (10) существует такое число $\mu_0 > 0$, что $o_\mu(1) < \min\{d, 1\}, \forall \mu \in (0, \mu_0]$. Следовательно, на множестве $[t_0, t_1^*] \setminus \bigcup_{i=1}^p [\tau_i - l, \tau_i + l]$ нет корней функции $\psi'_\mu(\tau)b$. Тогда из (12) с учетом (11) получим

$$|\tau_{\mu i} - \tau_i| \leq k_i \sqrt{\frac{k_i! o_\mu(1)}{|\psi^{(k_i)'}(\tau)b|}} \leq \sqrt{\frac{k_i! o_\mu(1)}{h}} \leq D \sqrt{o_\mu(1)},$$

где $\tau_{\mu i}$ – корень функции $\psi'_\mu(\tau)b$; $D = \max_{i=\overline{1, m}} k_i \sqrt{\frac{k_i!}{n}}, k = \max_{i=\overline{1, m}} \{k_i\}$.

Таким образом, $\int_{t_0}^t |u^0(\tau) - u^{*0}(\tau)| d\tau \leq 2pD \sqrt{o_\mu(1)}$ и неравенство (9) можно записать в виде

$$\|x^0(t) - x(t, u^{*0})\| \leq 2D \|b\| p e^{L(t_1^* - t)} \sqrt{o_\mu(1)}. \quad (13)$$

На основании вышеизложенного имеет место следующая теорема.

Теорема. Пусть u^0, u^{*0} – оптимальные управления в задачах (1), (2) соответственно, $x(\cdot, u), x^*(\cdot, u)$ – решения основной и усредненной систем, соответствующих допустимому в задаче (2) управлению. Тогда найдутся такие числа $\mu_0 > 0$ и $C > 0$, что справедливы оценки:

$$1) |J(u^0) - J(u)| \leq J_1(u^{*0}) - J_1(u) + C \sqrt{\mu} + \|A_\mu - A\|, \quad (14)$$

$$2) \|Hx(t_1^*, u) - q\| \leq C(\mu + \|A_\mu - A\|), \quad \forall \mu \in (0, \mu_0]. \quad (15)$$

Для доказательства теоремы достаточно заметить, что

$$|J(u^0) - J(u)| \leq |J_1(u^{*0}) - J_1(u)| + |J(u^0) - J(u^{*0})| + |J(u^{*0}) - J_1(u^{*0})| + |J(u) - J_1(u)|,$$

$$\|Hx(t_1^*, u) - q\| \leq \|Hx^*(t_1^*, u) - q\| + \|H\| \|x(t_1^*, u) - x^*(t_1^*, u)\|,$$

и воспользоваться оценками (7), (13).

Следствие. Предположим, что $A_\mu(t) = A + \mu A_1(t, \mu)$, где $A \in \mathbb{R}_{n,n}$, $\forall \mu \in (0, \mu_0]$.
В этом случае оценки (14), (15) допускают следующие уточнения:

$$1) \left| J(u^0) - J(u) \right| \leq J_1(u^{*0}) - J_1(u) + C\sqrt[k]{\mu};$$

$$2) \|Hx(t_1^*, u) - q\| \leq C\mu.$$

Библиографические ссылки

1. Крахотко ВВ. Оптимизация динамических систем управления с быстроменяющимися параметрами. *Доклады Академии наук Белорусской ССР*. 1990;34(7):592–595.
2. Крахотко ВВ, Павлов ВВ. Оптимизация нестационарной линейной системы с быстроменяющимися параметрами. *Вестник БГУ. Серия 1. Физика. Математика. Информатика*. 1987;2:54–57.
3. Боголюбов НН, Митропольский ЮА. *Асимптотические методы в теории нелинейных колебаний*. Москва: Физматлит; 1963. 407 с.
4. Беллман Р. *Теория устойчивости решений дифференциальных уравнений*. Москва: Издательство иностранной литературы; 1954. 216 с.
5. Понтрягин ЛС, Болтянский ВГ, Гамкрелидзе РВ, Мищенко ЕФ. *Математическая теория оптимальных процессов*. Москва: Наука; 1978. 392 с.

References

1. Krakhotko VV. [Optimization of dynamic control systems with changing parameters]. *Doklady Akademii nauk Belorusskoi SSR*. 1990;34(7):592–595. Russian.
2. Krakhotko VV, Pavlov VV. [Optimization of linear control systems with changing parameters]. *Vestnik BGU. Seriya 1. Fizika. Matematika. Informatika*. 1987;2:54–57. Russian.
3. Bogolyubov NN, Mitropol'skii YuA. *Asimptoticheskie metody v teorii nelineinykh kolebaniy* [Asymptotic methods in the theory of nonlinear oscillations]. Moscow: Fizmatlit; 1963. 407 p. Russian.
4. Bellman R. *Stability theory of differential equations*. New York: McGraw-Hill Book Company; 1953. 179 p.
Russian edition: Bellman R. *Teoriya ustoichivosti reshenii differentsial'nykh uravnenii*. Moscow: Izdatel'stvo inostrannoi literatury; 1954. 216 p.
5. Pontryagin LS, Boltyanskii VG, Gamkrelidze RV, Mishchenko EF. *Matematicheskaya teoriya optimal'nykh protsessov* [Mathematical theory of optimal processes]. Moscow: Nauka; 1978. 392 p. Russian.

Статья поступила в редколлегию 24.01.2020.
Received by editorial board 24.01.2020.

ЮБИЛЕИ

JUBILEES



**Юрий Семенович
ХАРИН**

**Yuriy Semenovich
KHARIN**

Исполнилось 70 лет доктору физико-математических наук, профессору, члену-корреспонденту НАН Беларуси директору НИИ прикладных проблем математики и информатики БГУ Юрию Семеновичу Харину и 50 лет с начала его научной и педагогической деятельности.

Юрий Семенович родился 17 сентября 1949 г. в с. Зырянское Томской области. В 1966 г. окончил школу в Томске с золотой медалью, в 1971 г. – Томский государственный университет с отличием, в 1974 г. – аспирантуру факультета прикладной математики с досрочной защитой кандидатской диссертации.

В связи с организацией в БГУ кафедры теории вероятностей и математической статистики в 1976 г. приглашен для работы на факультете прикладной математики в должности доцента. Здесь Ю. С. Харин состоялся как ученый и педагог, пройдя путь от доцента до заведующего кафедрой и директора института. В 1986 г. в Институте прикладной математики имени М. В. Келдыша АН СССР (Москва) он защитил докторскую диссертацию на тему «Статистический анализ и распознавание временных рядов, порожденных символьными последовательностями». В 1988 г. ему присвоено ученое звание профессора, в 2004 г. избран членом-корреспондентом НАН Беларуси.

По инициативе Юрия Семеновича в 1988 г. на факультете прикладной математики и информатики организована новая кафедра математического моделирования и анализа данных, которую он возглавлял со дня основания до 2018 г., а в настоящее время является ее научным руководителем. В 2000 г. Ю. С. Харин также инициировал создание в БГУ Национального научно-исследовательского центра прикладных проблем математики и информатики, преобразованного в 2008 г. в НИИ прикладных проблем математики и информатики, на который постановлением Совета Министров Республики Беларусь возложена координация в стране научных исследований по криптографии и анализу данных.

Юрий Семенович – признанный в Беларуси и за рубежом ученый в области прикладной математики и информатики. Основные направления его научных исследований – математическая и прикладная статистика, многомерный статистический анализ, распознавание и прогнозирование сложных случайных процессов, анализ данных, статистическое моделирование, криптография, защита информации.

На основе разработанных Ю. С. Хариним теории робастного (устойчивого) статистического распознавания образов, теории робастного статистического анализа данных и прогнозирования

построены новые минимаксно устойчивые (к искажениям вероятностной модели наблюдений) алгоритмы распознавания образов, идентификации и прогнозирования, которые гарантируют наименьшее отклонение риска на заданных параметрических и непараметрических семействах искажений, реализованы в пакетах прикладных программ, используемых в Беларуси, России, Германии, Южной Корее, и позволяют решать важные прикладные задачи внедрения информационных технологий в промышленности, медицине, экономике.

Юрию Семеновичу принадлежит ведущая роль в создании и развитии белорусской научной школы по криптологии – науке о математических и компьютерных методах защиты информации. С 2001 г. он является научным руководителем государственной программы по криптологии. В рамках государственных научных и научно-технических программ под его личным руководством выполнено более 50 научно-исследовательских работ, результаты которых имеют приоритетное значение и внедрены при создании компьютерных систем защиты информации в электронном документообороте страны.

Достижения Ю. С. Харина как ученого широко известны в нашей стране и за ее пределами и отражены в более чем 600 научных трудах, в том числе 5 индивидуальных монографиях, 2 из которых изданы за рубежом, 3 коллективных иностранных монографиях, 27 учебниках и учебных пособиях (среди них 14 – с грифом Министерства образования Республики Беларусь); он – соавтор международного издания «Encyclopedia of Statistical Sciences». Статьи Юрия Семеновича опубликованы в таких престижных зарубежных журналах, как «Mathematical Methods of Statistics», «Journal of Statistical Planning and Inference», «Applied Stochastic Models and Data Analysis», «Journal of Classification», «Communications in Statistics», «Pattern Recognition Letters», «Lecture Notes in Computer Science», «Lecture Notes in Statistics», «Теория вероятностей и ее применения», «Дискретная математика». Ю. С. Харин делал доклады более чем на 90 международных научных конференциях. Был приглашенным профессором в калифорнийских университетах (Беркли, Фресно) (США), Байрёйтском и Дрезденском университетах (Германия), Лейстерском университете (Великобритания), Венском университете (Австрия) и других ведущих научных центрах. Подготовил 34 кандидата и 1 доктора наук.

Юрий Семенович создал известную за рубежом научную школу «Математическое моделирование сложных систем, процессов защиты информации и компьютерного анализа данных». Он является организатором новых для Беларуси университетских специальностей «компьютер-

ная безопасность», «прикладная криптография», «экономическая кибернетика», двух специализаций по прикладной математике, магистратуры по специальности «компьютерный анализ данных», а также аспирантуры и докторантуры по специальности «методы и системы защиты информации, информационная безопасность».

Ю. С. Харин – член президиума ВАК Республики Беларусь, Белорусского математического общества, Белорусской ассоциации по анализу и распознаванию изображений, Американского математического общества, Международного института математической статистики, Международной ассоциации вычислительной техники, Европейской ассоциации обработки сигналов, Общества по математической статистике и теории вероятностей имени Бернулли, Белорусской статистической ассоциации (ее организатор и в 1998–2008 гг. – руководитель), редколлегии 6 зарубежных научных журналов и 5 республиканских. Он – редактор 25 сборников научных статей, заместитель главного редактора периодического межведомственного научного сборника «Проблемы защиты информации», организатор 12 международных научных конференций «Computer Data Analysis and Modeling», председатель программного комитета 14 международных конференций «Комплексная защита информации». Является главным редактором научного периодического издания «Журнал Белорусского государственного университета. Математика. Информатика».

Ю. С. Харин – заслуженный деятель науки Республики Беларусь (2010), лауреат Государственной премии Республики Беларусь в области науки и техники (2002), отличник образования Республики Беларусь (1999), лауреат премии имени А. Н. Севченко (1997), заслуженный работник БГУ (2013), награждался почетными грамотами Совета Министров Республики Беларусь, ВАК Республики Беларусь, Государственного комитета по науке и технологиям Республики Беларусь, Министерства образования Республики Беларусь, НАН Беларуси, БГУ.

Юрий Семенович – трудолюбивый, дисциплинированный, требовательный к себе и другим, доброжелательный, скромный человек, способный организовать коллектив. Сердечно поздравляем юбиляра и желаем ему крепкого здоровья, счастья, дальнейших творческих успехов в научной, педагогической и общественной деятельности.

*Факультет прикладной математики и информатики,
механико-математический факультет,
НИИ прикладных проблем математики и информатики,
редколлегия издания «Журнал Белорусского государственного
университета. Математика. Информатика»*



Валерий Александрович ЕРОВЕНКО

Valerii Aleksandrovich EROVENKO

Исполнилось 70 лет профессору кафедры общей математики и информатики механико-математического факультета БГУ доктору физико-математических наук, профессору Валерию Александровичу Еровенко.

В. А. Еровенко родился 2 марта 1950 г. в Кирове (Россия). В 1972 г. окончил факультет прикладной математики БГУ, а затем успешно завершил учебу в аспирантуре кафедры теории функций и функционального анализа механико-математического факультета. Начиная с 1975 г., после окончания аспирантуры, работал ассистентом, доцентом и профессором кафедры функционального анализа этого факультета. С 2003 по 2019 г. возглавлял кафедру общей математики и информатики механико-математического факультета БГУ. В 1995 г. Валерий Александрович первым представил и затем успешно защитил докторскую диссертацию в открытом при БГУ совете по защите диссертаций по математике. Оппонирующей организацией был Международный математический центр имени Стефана Банаха Института математики Польской академии наук. Докторская диссертация В. А. Еровенко на тему «Спектральные и фредгольмовы свойства линейных операторов в банаховых пространствах» посвящена исследованию устойчивости существенных спектров для различных классов ограниченных и дифференциальных операторов в банаховых пространствах.

В математических исследованиях В. А. Еровенко получены обобщения классической теоремы Вейля о существенном спектре на новые специальные классы линейных операторов, являющиеся исчерпывающими для рассматриваемых операторов. Решены известные задачи теории существенных спектров о совпадении последних и спектра квазиподобных операторов, а также о непрерывности спектра и существенных спектров ограниченных линейных операторов. Впервые в максимальной общности найдены точные формулы и выявлены

общие закономерности для всех существенных спектров различных классов обыкновенных дифференциальных операторов в широкой шкале лебеговых пространств. Это позволило доказать новые теоремы об инвариантности существенных спектров для обыкновенных дифференциальных операторов, обобщающие классическую теорему Вейля. Профессор В. А. Еровенко до сих пор активно занимается научными исследованиями, например руководит работой по научно-исследовательской теме «Аналитические методы в задачах устойчивости операторов и отображение математических моделей на архитектуру вычислительных систем».

В. А. Еровенко – крупный ученый, автор более 430 научных и научно-методических работ, включая 175 статей в журналах, монографии и учебные пособия, среди которых – «Функциональный анализ: спектральные и фредгольмовы свойства линейных операторов» и «Введение в теорию существенных спектров линейных операторов в банаховых пространствах». Валерий Александрович первым в Республике Беларусь начал активную философско-методологическую и практически ориентированную работу по созданию, апробации и внедрению университетских курсов лекций по «понимаемой высшей математике» для студентов гуманитарных специальностей. В частности, он разработал и опубликовал «Основы высшей математики для филологов» – оригинальный учебно-методический университетский курс лекций по математическим методам в лингвистике и теории стихосложения, а также учебно-методические пособия «Избранные главы курса “Основы высшей математики” для философов», «Основы высшей математики для студентов-международников в примерах и задачах». Валерий Александрович долгое время читал пользующийся большим успехом у студентов специальный авторский курс «Основы высшей математики для юристов». Все эти курсы связаны со специализацией студентов БГУ

и показывают возможность применения математических методов в сфере их будущей профессиональной деятельности.

С помощью критически-рефлексивного стиля математического мышления В. А. Ерошенко исследует различные актуальные проблемы философии математического образования. О широте его интересов можно, например, судить по отдельным журнальным публикациям последнего времени: «Существенные спектры обыкновенных дифференциальных операторов. I. Возмущения операторов» (Математические структуры и моделирование. 2019. № 1); «Социальный процесс “макдональдизации” на примере трансформации математического образования» (Alma mater. 2019. № 1); «Математическая психология и психология математики в университетском “дизайне психологического образования”» (Высшая школа. 2019. № 2); «Философская рефлексия экономических исследований: когнитивный, математический, информационный аспекты» (Российский гуманитарный журнал. 2019. Т. 8, № 4); «Когнитивные технологии обучения математике в инновационном географическом образовании» (Инновации в образовании. 2019. № 9); «Существенные спектры обыкновенных дифференциальных операторов. II. Устойчивость спектров» (Математические структуры и моделирование. 2020. № 1); «Философский дискурс “многомерности туризма”: географический, экономический и культурологический аспекты» (Высшая школа. 2020. № 1).

В период заведования кафедрой общей математики и информатики В. А. Ерошенко организовал методическую работу по созданию курсов лекций и учебно-методических пособий по высшей математике и информатике для студентов естественно-научных и гуманитарных факультетов с учетом специфики специальностей, для которых они предназначены. В это время на кафедре общей математики и информатики впервые стали разрабатываться не общие для всех студентов университета различных специальностей естественно-научного или гуманитарного профиля курсы высшей математики, а лекционные курсы, привязанные к соответствующим специальностям. Как заведующий, Валерий Александрович стимулировал сотрудников кафедры к написанию статей и тезисов по методике преподавания высшей математики для специальностей тех факультетов, на которых они работали. Итоги учебной и методической работы последнего десятилетия кафедры общей математики и информатики были представлены на международных научно-практических конференциях «Ма-

тематика и информатика в естественно-научном и гуманитарном образовании» (2012) и «Методология и философия преподавания математики и информатики» (2015). В. А. Ерошенко был ответственным редактором сборников материалов этих конференций с представительным участием российских ученых.

Под руководством В. А. Ерошенко защищены 3 кандидатские диссертации, а теперь профессор вносит свой посильный вклад в подготовку педагогических и научных кадров, являясь членом докторского совета по защите диссертаций по математике при БГУ.

Валерий Александрович – высокопрофессиональный педагог и интересный лектор, преподаватель, умеющий убедить слушателя в обоснованности математических утверждений, универсальности и эффективности методов математики. Его лекции неизменно пользуются успехом у студентов. Огромный профессиональный опыт, мудрость, тонкое чутье и понимание своих коллег позволяют Валерию Александровичу найти нужные и важные слова для поддержки в трудные минуты, создания комфортной рабочей обстановки. Талант и яркая индивидуальность профессора проявляются не только в работе, но и в других сферах жизни. Ему присущи жизнелюбие и оптимизм, хорошее чувство юмора, он приятный и интересный собеседник. Валерий Александрович – человек разносторонний, любит литературу, музыку, театр. Благодаря научному и педагогическому таланту, высокой культуре общения и доброжелательности он снискал уважение и авторитет среди коллег и студентов. Профессор В. А. Ерошенко награжден грамотами и почетными грамотами БГУ, ВАК Республики Беларусь, Министерства образования Республики Беларусь. Он имеет почетные звания «Отличник образования» и «Заслуженный работник БГУ».

Сердечно поздравляем Валерия Александровича с 70-летием и желаем ему крепкого здоровья, счастья, дальнейших творческих успехов в научной, педагогической и общественной деятельности.

*В. В. Амелькин, И. В. Белько, В. И. Берник,
В. В. Беняш-Кривец, С. М. Босяков, М. К. Буза,
В. М. Волков, А. Д. Егоров, Э. И. Зверович,
Н. И. Изобов, Н. С. Коваленко, В. И. Корзюк,
В. Г. Кротов, А. В. Лебедев, Д. Г. Медведев,
О. И. Мельников, В. Н. Русак, С. А. Самаль,
Л. А. Янович, В. И. Янчевский, О. В. Гулина,
М. В. Мартон, О. М. Матейко,
В. А. Прокашева, Н. Б. Яблонская*

ПАМЯТИ УЧЕНОГО

TO THE MEMORY OF SCIENTIST



**Регина Иосифовна
ТЫШКЕВИЧ**

**Regina Iosifovna
TYSHKEVICH**

17 ноября 2019 г. ушла из жизни Регина Иосифовна Тышкевич – один из самых авторитетных педагогов БГУ, выдающийся белорусский математик, доктор физико-математических наук, профессор.

Регина Иосифовна родилась 20 октября 1929 г. в Минске. С началом войны в 1941 г. юная Регина с мамой Марисей Ивановной были эвакуированы в Ижевск (Удмуртия). В этот суровый период тыловой жизни Мария Ивановна работала на оборонном заводе, а дочь помогала по дому и училась в школе. По счастливой случайности в эти места для работы в школе были эвакуированы лучшие учителя математики из Ленинграда, которые показали Регине красоту этой науки и фактически определили ее дальнейшую судьбу.

В 1946 г. Регина вернулась в Беларусь одна, так как ее мать не отпустили с завода из-за нехватки рабочих рук. Она остановилась у своей тети в уютном городке Вилейка. В 1947 г. Регина окончила с золотой медалью школу и поступила на физико-математический факультет БГУ, который окончила с отличием в 1952 г. Затем – учеба в аспирантуре. В 1956 г. она стала преподавать на родном факультете.

В то же самое время Р. И. Тышкевич связала свою жизнь с Д. А. Супруненко. Будучи великим ученым, одним из основателей белорусской алгебраической школы и впоследствии фактически

ставшим создателем белорусской математической кибернетики, он оказал огромное влияние на научные интересы Регины Иосифовны. Под его руководством в 1959 г. она защитила кандидатскую диссертацию по исследованию нильпотентных групп.

Вскоре центр научных интересов Р. И. Тышкевич сместился от алгебры в сторону дискретной математики, и в особенности к одному из стремительно развивающихся и перспективных ее направлений – комбинаторике и теории графов. Впрочем, алгебра не прекращала оказывать значительное влияние на научные взгляды Регины Иосифовны. И отличительной чертой всего ее дальнейшего творчества являлись как раз сочетание, синтез комбинаторных и алгебраических методов в исследовании.

В 1984 г. в Институте кибернетики имени В. М. Глушкова АН УССР (Киев) Регина Иосифовна защитила диссертацию на тему «Алгебраические методы теории графов», ставшую первой в Советском Союзе докторской диссертацией по теории графов. В 1986 г. Регине Иосифовне присвоено ученое звание профессора.

Р. И. Тышкевич – основатель белорусской научной школы по теории графов, занимающей лидирующие позиции в рамках бывшего СССР и имеющей признание в дальнем зарубежье. В этой области Регине Иосифовне принадлежит ряд результатов мирового уровня. Главный из них – разработка тео-

рии алгебраической декомпозиции графов. Сами по себе декомпозиционные методы применялись в теории графов и ранее. Новизной декомпозиции Р. И. Тышкевич является ее алгебраичность. При этом множество графов превращаются в алгебраическую систему с действующей на ней полугруппой операторов. Умножение в полугруппе теоретикоматематическое: операторы перемножаются как морфизмы. Грубо говоря, операторами служат сами графы. В общей алгебре – это старая испытанная идея, в теории графов – явление новое. Результат указанных построений есть декомпозиция произвольного графа на части, в чем-то напоминающая каноническое разложение натурального числа. Разработанная Р. И. Тышкевич теория алгебраической декомпозиции графов позволила получить ряд впечатляющих результатов. В частности, была решена проблема полной характеристики множества униграфов, которая оставалась открытой более 30 лет. В последние годы с помощью алгебраической декомпозиции графов сделаны существенные продвижения в исследовании известных открытых гипотез теории графов, таких как гипотеза реконструируемости Келли – Улама (1941) или гипотеза Хартсфилда – Рингеля об антиматематичности (1990).

Большой вклад внесла Регина Иосифовна в теорию представлений графов в виде графов пересечений ребер гиперграфов. В частности, ею введено понятие реберного гиперграфа, являющееся обобщением понятий реберного графа и двойственного гиперграфа, и для этого нового объекта доказаны аналоги классических теорем Уитни и Берга. Получены значимые результаты в решении проблемы нахождения степенного порога полиномиальной разрешимости для задачи распознавания графов пересечений ребер линейных 3-униформных гиперграфов, что служит одним из возможных подходов к решению известной задачи Ловаса о характеристике графов пересечений ребер 3-униформных гиперграфов. Существенна роль Р. И. Тышкевич в развитии теорий изоморфизма графов, степенных последовательностей, матроидной декомпозиции.

Регина Иосифовна на протяжении последних десятилетий являлась научным руководителем при выполнении заданий государственных программ научных исследований, была научным координатором белорусских групп из БГУ и Института математики НАН Беларуси, выполнявших

исследования в рамках совместных международных научно-исследовательских проектов ИНТАС и Правительства Республики Беларусь по близкой тематике.

Р. И. Тышкевич – автор около 150 научных и научно-методических работ, в том числе 10 учебников и монографий, 3 из которых переведены на английский язык и изданы за рубежом, а некоторые выдержали несколько переизданий.

Большой вклад Р. И. Тышкевич внесла в подготовку кадров высшей квалификации. Она являлась членом советов по защите кандидатских и докторских диссертаций Объединенного института проблем информатики и Института математики НАН Беларуси, а также научного совета по государственной программе фундаментальных исследований. Регина Иосифовна подготовила 17 кандидатов и 1 доктора наук. Все ученики помнят ее лекции, в которых глубина, методическая точность и доступность сочетались с высокой культурой, увлеченностью и личным обаянием.

Заслуги и достижения Р. И. Тышкевич были по достоинству отмечены государством. В 1992 г. ей присвоено высокое звание «Заслуженный работник народного образования Республики Беларусь». В 1998 г. за книгу «Лекции по теории графов», вышедшую в 1990 г. в издательстве «Наука» (Москва), Регина Иосифовна совместно с соавторами удостоена Государственной премии Республики Беларусь. В 2009 г. Указом Президента Республики Беларусь Регине Иосифовне вручена одна из высших наград работников науки и культуры – медаль Франциска Скорины.

Р. И. Тышкевич была человеком высокой культуры и эрудиции, ее интересы никогда не ограничивались одной лишь математикой. Она живо интересовалась вопросами литературы и истории, театральным искусством, великолепно разбиралась в поэзии. Регина Иосифовна всегда принимала активное участие в общественной и культурной жизни родного факультета.

С уходом профессора Р. И. Тышкевич коллектив механико-математического факультета, кафедры математической кибернетики потерял высококвалифицированного лектора, педагога, выдающегося ученого, математика и простого, искреннего, неравнодушного и доброжелательного коллегу. Светлая память о Регине Иосифовне навсегда сохранится в наших сердцах.

Коллеги и ученики

АННОТАЦИИ ДЕПОНИРОВАННЫХ В БГУ РАБОТ INDICATIVE ABSTRACTS OF THE PAPERS DEPOSITED IN BSU

УДК 517.926.4(075.8)

Кононова О. А. **Линейные однородные дифференциальные уравнения с переменными коэффициентами и основные методы их решения** [Электронный ресурс] : учеб.-метод. разработка / О. А. Кононова, Н. И. Ильинкова, Н. К. Филиппова ; БГУ. Электрон. текстовые дан. Минск, 2019. 18 с. Библиогр.: с. 17. Режим доступа: <http://elib.bsu.by/handle/123456789/235107>. Загл. с экрана. Деп. 04.12.2019, № 011704122019.

Учебно-методическая разработка содержит теоретические сведения о методах нахождения фундаментальных решений при помощи замены независимой переменной и искомой функции. Представлены типовые примеры с подробным описанием их решения.

УДК 51(075.8)

Велько О. А. **Основы высшей математики** [Электронный ресурс] : электрон. учеб.-метод. комплекс для спец. 1-21 02 01 «Философия» / О. А. Велько, Н. А. Моисеева ; БГУ. Электрон. текстовые дан. Минск, 2020. 105 с. : ил. Библиогр.: с. 103–105. Режим доступа: <http://elib.bsu.by/handle/123456789/241076>. Загл. с экрана. Деп. 05.03.2020, № 002005032020.

Электронный учебно-методический комплекс по учебной дисциплине «Основы высшей математики» предназначен для студентов специальности 1-21 02 01 «Философия». Он включает лекционный материал, планы семинарских занятий, примерные задания для управляемой самостоятельной работы студентов, примерные тестовые задания, примерную итоговую контрольную работу, задания эвристического типа, вопросы для подготовки к зачету, примерный тематический план, содержание учебного материала, список литературы.

УДК 51(075.8)

Велько О. А. **Основы высшей математики** [Электронный ресурс] : электрон. учеб.-метод. комплекс для спец. 1-23 01 05 «Социология» / О. А. Велько, Н. А. Моисеева ; БГУ. Электрон. текстовые дан. Минск, 2020. 257 с. : ил. Библиогр.: с. 255–257. Режим доступа: <http://elib.bsu.by/handle/123456789/241078>. Загл. с экрана. Деп. 05.03.2020, № 002105032020.

Электронный учебно-методический комплекс по учебной дисциплине «Основы высшей математики» предназначен для студентов специальности 1-23 01 05 «Социология». Он включает лекционный материал, задания для практических занятий, примерные задания для управляемой самостоятельной работы студентов, тестовые задания, контрольные работы, задания эвристического типа, вопросы для подготовки к экзамену, примерный тематический план, содержание учебного материала, список литературы.

УДК 51(075.8)

Моисеева Н. А. **Основы высшей математики** [Электронный ресурс] : электрон. учеб.-метод. комплекс для спец. 1-23 01 15 «Социальные коммуникации» / Н. А. Моисеева, О. А. Велько ; БГУ. Электрон. текстовые дан. Минск, 2020. 193 с. : ил. Библиогр.: с. 191–193. Режим доступа: <http://elib.bsu.by/handle/123456789/241081>. Загл. с экрана. Деп. 05.03.2020, № 002205032020.

Электронный учебно-методический комплекс по учебной дисциплине «Основы высшей математики» предназначен для студентов специальности 1-23 01 15 «Социальные коммуникации». Он включает лекционный материал, задания для практических занятий, примерные задания для управляемой самостоятельной работы студентов, тестовые задания, контрольные работы, задания эвристического типа, вопросы для подготовки к зачету, примерный тематический план, содержание учебного материала, список литературы.

СОДЕРЖАНИЕ

ВЕЩЕСТВЕННЫЙ, КОМПЛЕКСНЫЙ И ФУНКЦИОНАЛЬНЫЙ АНАЛИЗ

<i>Бондарев С. А.</i> Вложение класса Хайлаша – Соболева $M_{\alpha}^p(X)$ в пространство непрерывных функций в критическом случае.....	6
---	---

МАТЕМАТИЧЕСКАЯ ЛОГИКА, АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

<i>Кондратёнок Н. В.</i> Анализ RSA-криптосистемы в абстрактных числовых кольцах	13
--	----

ГЕОМЕТРИЯ И ТОПОЛОГИЯ

<i>Кукрак Г. О., Тимохович В. Л.</i> О непрерывности функторов вида $C(X, Y)$	22
---	----

ДИФФЕРЕНЦИАЛЬНЫЕ УРАВНЕНИЯ И ОПТИМАЛЬНОЕ УПРАВЛЕНИЕ

<i>Устилко Е. В., Ломовцев Ф. Е.</i> Условия согласования значений характеристической кривой производной на конце струны, начальных данных и правой части волнового уравнения	30
---	----

ТЕОРЕТИЧЕСКАЯ И ПРИКЛАДНАЯ МЕХАНИКА

<i>Бауэр С. М., Воронкова Е. Б.</i> Влияние условий закрепления на появление несимметричных форм равновесия у круглых пластин под действием нормального давления	38
<i>Королевич В. В.</i> Решение неосесимметричной стационарной задачи теплопроводности для полярно-ортотропной кольцевой пластины переменной толщины с учетом теплообмена с внешней средой	47

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ

<i>Шарыкин Р. Е., Курбацкий А. Н.</i> Применение формальных методов при проектировании коллаборационной системы противовирусной защиты	59
--	----

КРАТКИЕ СООБЩЕНИЯ

<i>Волошко В. А., Вечерко Е. В.</i> Новые верхние границы для функции нецентрального хи-квадрат распределения	70
<i>Крахотко В. В., Размыслович Г. П., Горячкин В. В.</i> Оптимизация линейной динамической системы с периодическими быстроменяющимися коэффициентами.....	75

ЮБИЛЕИ

Юрий Семенович Харин	80
Валерий Александрович Ерошенко.....	82

ПАМЯТИ УЧЕНОГО

Регина Иосифовна Тышкевич	84
Аннотации депонированных в БГУ работ.....	86

CONTENTS

REAL, COMPLEX AND FUNCTIONAL ANALYSIS

<i>Bondarev S. A.</i> Inclusion of Hajlasz – Sobolev class $M_\alpha^p(X)$ into the space of continuous functions in the critical case.....	6
---	---

MATHEMATICAL LOGIC, ALGEBRA AND NUMBER THEORY

<i>Kondratyionok N. V.</i> Analysis of the RSA-cryptosystem in abstract number rings.....	13
---	----

GEOMETRY AND TOPOLOGY

<i>Kukrak H. O., Timokhovich V. L.</i> On the continuity of functors of the type $C(X, Y)$	22
--	----

DIFFERENTIAL EQUATIONS AND OPTIMAL CONTROL

<i>Ustilko E. V., Lomovtsev F. E.</i> Matching conditions for values of characteristic oblique derivative at the end of a string, initial data and right-hand side of the wave equation	30
---	----

THEORETICAL AND PRACTICAL MECHANICS

<i>Bauer S. M., Voronkova E. B.</i> Influence of boundary constraints on the appearance of asymmetrical equilibrium states in circular plates under normal pressure	38
<i>Karalevich U. V.</i> Solution of nonaxisymmetric stationary problem of heat conductivity for polar-orthotropic ring plate of variable thickness with account of heat transfer with external environment.....	47

THEORETICAL FOUNDATIONS OF COMPUTER SCIENCE

<i>Sharykin R. E., Kourbatski A. N.</i> Application of formal methods in the design of a collaborative virus defense system	59
---	----

SHORT COMMUNICATIONS

<i>Voloshko V. A., Vecherko E. V.</i> New upper bounds for noncentral chi-square cdf.....	70
<i>Krakhotko V. V., Razmyslovich G. P., Goryachkin V. V.</i> Optimization of a linear dynamic system with periodic changing parameters	75

JUBILEES

Yuriy Semenovich Kharin.....	80
Valerii Aleksandrovich Erovenko	82

TO THE MEMORY OF SCIENTIST

Regina Iosifovna Tyshkevich	84
Indicative abstracts of the papers deposited in BSU.....	86

Журнал включен Высшей аттестационной комиссией Республики Беларусь в Перечень научных изданий для опубликования результатов диссертационных исследований по физико-математическим наукам (в области математики и информатики).

Журнал включен в библиографические базы данных научных публикаций «Российский индекс научного цитирования» (РИНЦ), Mathematical Reviews, Ulrichsweb, Google Scholar, zbMath.

**Журнал Белорусского
государственного университета.
Математика. Информатика.
№ 1. 2020**

Учредитель:
Белорусский государственный университет

Юридический адрес: пр. Независимости, 4,
220030, г. Минск.

Почтовый адрес: пр. Независимости, 4,
220030, г. Минск.

Тел. (017) 259-70-74, (017) 259-70-75.

E-mail: jmathinf@bsu.by

URL: <https://journals.bsu.by/index.php/mathematics>

«Журнал Белорусского государственного
университета. Математика. Информатика»
издается с января 1969 г.
До 2017 г. выходил под названием «Вестник БГУ.
Серия 1, Физика. Математика. Информатика»
(ISSN 1561-834X).

Редактор *Т. Р. Джум*
Технический редактор *В. В. Пишкова*
Корректор *Л. А. Меркуль*

Подписано в печать 31.03.2020.
Тираж 105 экз. Заказ 121.

Республиканское унитарное предприятие
«Информационно-вычислительный центр
Министерства финансов Республики Беларусь».
ЛП № 02330/89 от 03.03.2014.
Ул. Кальварийская, 17, 220004, г. Минск.

© БГУ, 2020

**Journal
of the Belarusian State University.
Mathematics and Informatics.
No. 1. 2020**

Founder:
Belarusian State University

Registered address: 4 Niezaliežnasci Ave.,
Minsk 220030.

Correspondence address: 4 Niezaliežnasci Ave.,
Minsk 220030.

Tel. (017) 259-70-74, (017) 259-70-75.

E-mail: jmathinf@bsu.by

URL: <https://journals.bsu.by/index.php/mathematics>

«Journal of the Belarusian State University.
Mathematics and Informatics»
published since January, 1969.
Until 2017 named «Vestnik BGU.
Seriya 1, Fizika. Matematika. Informatika»
(ISSN 1561-834X).

Editor *T. R. Dzhum*
Technical editor *V. V. Pishkova*
Proofreader *L. A. Merkul'*

Signed print 31.03.2020.
Edition 105 copies. Order number 121.

Republican Unitary Enterprise
«Informatsionno-vychislitel'nyi tsentr
Ministerstva finansov Respubliki Belarus'».
License for publishing No. 02330/89, 3 March 2014.
17 Kal'varyjskaja Str., Minsk 220004.

© BSU, 2020