Подписной индекс 80307
ISSN 2541-7525

ВЕСТНИК
САМАРСКОГО УНИВЕРСИТЕТА
ЕСТЕСТВЕННОНАУЧНАЯ СЕРИЯ

- *Математика*
- *Механика*
- *Физика*

ТОМ 27 • № 1 • 2021 ГОД

УЧРЕДИТЕЛЬ И ИЗДАТЕЛЬ ЖУРНАЛА
федеральное государственное автономное образовательное учреждение высшего образования
«Самарский национальный исследовательский университет имени академика С.П. Королева»
(Самарский университет)

eLIBRARY.RU РИНЦ ВИНИТИ ULRICH'S Periodical Directory Math-Net.ru zbMATH MathSciNet
Все статьи по тематике международной базы данных zbMATH считаются включенными в Перечень ведущих научных журналов Высшей аттестационной комиссии при Министерстве образования и науки РФ
Журнал издается с 1995 г. под названием «Вестник Самарского государственного университета», с 2016 г. — «Вестник Самарского университета. Естественнонаучная серия»

Главный редактор:
Е.В. Шахматов, член-корреспондент РАН, д-р тех. наук, проф., научный руководитель Самарского университета, главный научный сотрудник института акустики машин, зав. кафедрой автоматических систем энергетических установок (Самара, Самарский университет, РФ)

Заместители главного редактора:
А.Ф. Крутов, д-р физ.-мат. наук, проф., проф. кафедры общей и теоретической физики, зам. директора Межвузовского научно-исследовательского центра по теоретическому материаловедению (Самара, Самарский университет, РФ)
С.В. Асташкин, д-р физ.-мат. наук, проф., зав. кафедрой функционального анализа и теории функций (Самара, Самарский университет, РФ)
Л.В. Степанова, д-р физ.-мат. наук, доц., проф. кафедры математического моделирования в механике (Самара, Самарский университет, РФ)

Ответственный секретарь:
М.А. Лихобабенко, канд. физ.-мат. наук

Лит. редактирование, корректура
Т.А. Мурзиновой
Компьютерная верстка, макет
М.А. Лихобабенко
Выпускающий редактор
Т.А. Мурзинова
Информация на английском языке
М.С. Стрельникова

Издатель: Самарский университет
Адрес издателя:
443086, Российская Федерация, г. Самара,
Московское шоссе, 34, корп. 22а, 312 б.

Центр периодических изданий Самарского университета
Адрес редакции: 443011, Российская Федерация, г. Самара, ул. Акад. Павлова, 1.
E-mail: *nsvestnik@ssau.ru*
www: *http://journals.ssau.ru/index.php/vestnik-est*

Свидетельство о регистрации средства массовой информации **ПИ № ФС 77-67328** от 05.10.2016 г., выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций

Подписной индекс в каталоге
АО Агентство «Роспечать» 80307
ISSN 2541-7525

Авторские статьи не обязательно отражают мнение издателя.

0+

Цена свободная

Подписано в печать 17.04.2021.
Формат 60 × 84/8.
Бумага офсетная. Печать оперативная.
Печ. л. 14.
Тираж 200 экз. (первый завод — 30 экз.). Заказ №

Отпечатано в типографии Самарского университета
443086, Российская Федерация, г. Самара,
Московское шоссе, 34.
www: http://www.ssau.ru/info/struct/otd/common/edit

Редакционная коллегия:
В.Э. Видельман, д-р физ.-мат. наук, проф., зав. кафедрой экспериментальной механики и конструкционного материаловедения, директор Центра экспериментальной механики (Пермь, Пермский национальный исследовательский политехнический университет, РФ)
А.В. Горохов, д-р физ.-мат. наук, проф., проф. кафедры общей и теоретической физики (Самара, Самарский университет, РФ)
А.М. Зюзин, д-р физ.-мат. наук, проф., зав. кафедрой экспериментальной физики (Саранск, Национальный исследовательский Мордовский государственный университет им. Н.П. Огарева, РФ)
В.В. Ивахник, д-р физ.-мат. наук, проф., декан физического факультета, зав. кафедрой оптики и спектроскопии (Самара, Самарский университет, РФ)
А.И. Кожанов, д-р физ.-мат. наук, проф., ведущий научный сотрудник лаборатории теории функций (Новосибирск, Институт математики им. С.Л. Соболева Сибирского отделения РАН, РФ)
М.А. Леган, д-р тех. наук, доц., проф. кафедры прочности летательных аппаратов (Новосибирск, Новосибирский государственный технический университет, РФ)
Константин Панкрашкин, д-р физ.-мат. наук, проф. кафедры математики (Орсе, Университет Париж-юг 11, Франция)
А.Н. Панов, д-р физ.-мат. наук, проф., зав. кафедрой алгебры и геометрии (Самара, Самарский университет, РФ)
А.В. Покоев, д-р физ.-мат. наук, проф., зав. кафедрой физики твердого тела и неравновесных систем (Самара, Самарский университет, РФ)
Давиде М. Прозерпио, д-р химии, проф. кафедры химии (Милан, Миланский университет, Италия)
Л.С. Пулькина, д-р физ.-мат. наук, проф., проф. кафедры дифференциальных уравнений и теории управления (Самара, Самарский университет, РФ)
С.Г. Пятков, д-р физ.-мат. наук, проф., зав. кафедрой высшей математики; ведущий научный сотрудник (Ханты-Мансийск, Югорский государственный университет, РФ; Новосибирск, Институт математики им. С.Л. Соболева Сибирского отделения РАН, РФ)
В.В. Ревин, д-р биол. наук, проф., декан факультета биотехнологии и биологии, зав. кафедрой биотехнологии, биоинженерии и биохимии (Саранск, Национальный исследовательский Мордовский государственный университет им. Н.П. Огарева, РФ)
В.А. Салеев, д-р физ.-мат. наук, проф., проф. кафедры физики (Самара, Самарский университет, РФ)
В.А. Соболев, д-р физ.-мат. наук, проф., зав. кафедрой дифференциальных уравнений и теории управления, профессор кафедры кибернетики (Самара, Самарский университет, РФ)
П.А. Терехин, д-р физ.-мат. наук, проф., проф. кафедры теории функций и стохастического анализа (Саратов, Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского, РФ)
А.И. Хромов, д-р физ.-мат. наук, проф., проф. кафедры прикладной математики и информатики (Комсомольск-на-Амуре, Комсомольский-на-Амуре государственный университет, РФ)

© Самарский университет, 2021

Subscription Index 80307
ISSN 2541-7525

VESTNIK
OF SAMARA UNIVERSITY
NATURAL SCIENCE SERIES

- Mathematics
- Mechanics
- Physics

VOL. 27 • № 1 • 2021

JOURNAL FOUNDER AND PUBLISHER
Federal State Autonomous Educational Institution of Higher Education
«Samara National Research University»
(Samara University)

eLIBRARY.RU RSCI VINITI ULRICH'S Periodical Directory Math-Net.ru zbMATH MathSciNet
All articles on the subject of an international database zbMATH seemed to be included in the list of leading scientific journals of the Higher Attestation Committee at the Ministry of Education and Science of the Russian Federation
The journal is piblished since 1995 under the title Vestnik of Samara State University, since 2016 — Vestnik of Samara University. Natural Science Series

Chief editor:
E.V. Shakhmatov, corresponding member of the RAS, Dr. of Science (Engineering), prof., scientific adviser of Samara National Research University, chief researcher of Machine Acoustics Institute, head of Department of Power Plant Automatic Systems (Samara, Samara National Research University, RF)

Deputy chief editors:
A.F. Krutov, Dr. of Phys.-Math. Sci., prof., professor of Department of General and Theoretical Physics, deputy director of Samara Center for Theoretical Materials Science (Samara, Samara National Research University, RF)
S.V. Astashkin, Dr. of Phys.-Math. Sci., prof., head of the Department of Functional Analysis and Function Theory (Samara, Samara National Research University, RF)
L.V. Stepanova, Dr. of Phys.-Math. Sci., associate prof., prof. of the Department of Mathematical Modelling in Mechanics (Samara, Samara National Research University, Russian Federation)

Executive editor:
M.A. Likhobabenko, Cand. of Phys.-Math. Sci.

Literary editing, proofreading
T.A. Murzinova
Computer makeup, dummy
M.A. Likhobabenko
Executive editor
T.A. Murzinova
Information in English
M.S. Strelnikov

Publisher: Samara National Research University
Adress publisher:
312 b, building 22 a, 34, Moskovskoye shosse,
Samara, 443086, Russian Federation.

Centre of Periodical Publications of Samara University
Adress of editorial stuff: 1, Acad. Pavlov Street, Samara, 443011, Russian Federation.
E-mail: *nsvestnik@ssau.ru*
www: *http://journals.ssau.ru/index.php/vestnik-est*

Certificate of registration of means of mass media **ПИ № ФС 77-67328** dated 05.10.2016, issued by the Federal Service for Supervision of Communications, Information Technology and Mass Media.

Subscription Index in the Agency «Rospechat» 80307
ISSN 2541-7525

Author's articles do not necessarily reflect the views of the publisher.

0+

Price free

Passed for printing 17.04.2021.
Format 60 × 84/8.
Litho paper. Instant print.
Print. sheets 14.
Circulation 200 copies (first printing – 30 copies).
Order №

Printed on the printing house of Samara University
34, Moskovskoye shosse, Samara, 443086, Russian Federation
www: http://www.ssau.ru/info/struct/otd/common/edit

Editorial board:
V.E. Videlman, Dr. of Phys.-Math. Sci., prof., head of the Department of Experimental Mechanics and Engineering Materials Science, head of the Center of Experimental Mechanics (Perm, Perm National Research Polytechnic University, RF)
A.V. Gorokhov, Dr. of Phys.-Math. Sci., prof., prof. of the Department of General and Theoretical Physics (Samara, Samara National Research University, RF)
A.M. Zyuzin, Dr. of Phys.-Math. Sci., prof., head of the Department of Experimental Physics (Saransk, Ogarev Mordovia National University, RF)
V.V. Ivakhnik, Dr. of Phys.-Math. Sci., prof., dean of the Faculty of Physics, head of the Department of Optics and Spectroscopy (Samara, Samara National Research University, RF)
A.I. Kozhanov, Dr. of Phys.-Math. Sci., prof., leading research worker of the Laboratory of the Theory of Functions (Novosibirsk, Sobolev Institute of Mathematics of the Siberian branch of the RAS, RF)
M.A. Legan, Dr. of Enginering Sci., associate prof., prof. of the Department of Strength of Flying Machines (Novosibirsk, Novosibirsk State Technical University, RF)
Konstantin Pankrashkin, Dr. of Phys.-Math. Sci., prof. of the Department of Mathematics (Orsay, University of Paris-Sud 11, France)
A.N. Panov, Dr. of Phys.-Math. Sci., professor, head of the Department of Algebra and Geometry (Samara, Samara National Research University, RF)
A.V. Pokoev, Dr. of Phys.-Math. Sci., professor, head of the Department of Solid-State Physics and Nonequilibrium Systems (Samara, Samara National Research University, RF)
Davide M. Proserpio, Dr. of Chemistry, prof. of the Department of Chemistry (Milan, University of Milan, Italy)
L.S. Pulkina, Dr. of Phys.-Math. Sci., prof., prof. of the Department of Differential Equations and Control Theory (Samara, Samara National University, RF)
S.G. Pyatkov, Dr. of Phys.-Math. Sci., prof., head of the Department of Higher Mathematics; leading research worker (Khanty-Mansiysk, Yugra State University, RF; Novosibirsk, Sobolev Institute of Mathematics of the Siberian branch of the RAS, RF)
V.V. Revin, Dr. Degree in Biology, prof., dean of the Faculty of Biotechnology and Biology, head of the Department of Biotechnology, Bioengineering and Biochemistry (Saransk, Ogarev Mordovia National Research University, RF)
V.A. Saleev, Dr. of Phys.-Math. Sci., prof., prof. of the Department of Physics (Samara, Samara National Research University, RF)
V.A. Sobolev, Dr. of Phys.-Math. Sci., prof., head of the Department of Differential Equations and Control Theory, prof. of the Department of Engineering Cybernetics (Samara, Samara National Research University, RF)
P.A. Terekhin, Dr. of Phys.-Math. Sci., prof., prof. of the Department of Function Theory and Stochastic Analysis (Saratov, Saratov State University, RF)
A.I. Khromov, Dr. of Phys.-Math. Sci., prof., prof. of the Department of Applied Mathematics and Informatics (Komsomolsk-on-Amur, Komsomolsk-na-Amure State University, RF)

© Samara University, 2021

СОДЕРЖАНИЕ

Математика

Богатов А.В. Задача с динамическим нелокальным условием для одномерного гиперболического уравнения **7**
Дмитриев В.Б. Краевая задача с нелокальным граничным условием интегрального вида для многомерного уравнения IV порядка **15**
Providas E., Pulkina L.S., Parasidis I.N. Factorization of ordinary and hyperbolic integro-differential equations with integral boundary conditions in a Banach space **29**
Рацеев С.М., Лавриненко А.Д., Степанова Е.А. Об алгоритме Берлекэмпа — Месси и его применении в алгоритмах декодирования **44**
Рацеев С.М., Череватенко О.И., Чернявская В.А. О некоторых криптосистемах, основанных на алгебраических кодах **62**
Шамолин М.В. Задачи дифференциальной и топологической диагностики. Часть 6. Статистическое решение задачи дифференциальной диагностики **74**

Механика

Lychev S.A., Koifman K.G., Digilov A.V. Nonlinear dynamic equations for elastic micromorphic solids and shells. Part I **81**

Физика

Кузнецова А.А., Салеев В.А. Рождение изолированных фотонов с большими поперечными импульсами на БАК в реджевском пределе КХД **104**

Требования к оформлению статей **111**

CONTENTS

Mathematics

Bogatov A.V. A problem with nonlocal condition for one-dimensional hyperbolic equation **7**
Dmitriev V.B. A boundary value problem with a nonlocal boundary condition of integral form for a multidimensional equation of IV order **15**
Providas E., Pulkina L.S., Parasidis I.N. Factorization of ordinary and hyperbolic integro-differential equations with integral boundary conditions in a Banach space **29**
Ratseev S.M., Lavrinenko A.D., Stepanova E.A. On the Berlekamp — Massey algorithm and its application for decoding algorithms **44**
Ratseev S.M., Cherevatenko O.I., Chernyavskaya V.A. On some cryptosystems based on algebraic codes **62**
Shamolin M.V. Problems of differential and topological diagnostics. Part 6. Statistical solving of the problem of differential diagnostics **74**

Mechanics

Lychev S.A., Koifman K.G., Digilov A.V. Nonlinear dynamic equations for elastic micromorphic solids and shells. Part I **81**

Physics

Kuznetsova A.A., Saleev V.A. Production of isolated photons with large transverse momenta at LHC in the Regge limit of QCD **104**

Requirements to the design of articles **111**

МАТЕМАТИКА

Научная статья
DOI: 10.18287/2541-7525-2021-27-1-7-14

УДК 517.95

Дата: поступления статьи: 15.01.2021
после рецензирования: 17.02.2021
принятия статьи: 28.02.2021

А.В. Богатов
Самарский национальный исследовательский университет
имени академика С.П. Королева, г. Самара, Российская Федерация
E-mail: andrebogato@mail.ru. ORCID: https://orcid.org/0000-0001-5797-1930

ЗАДАЧА С ДИНАМИЧЕСКИМ НЕЛОКАЛЬНЫМ УСЛОВИЕМ ДЛЯ ОДНОМЕРНОГО ГИПЕРБОЛИЧЕСКОГО УРАВНЕНИЯ

АННОТАЦИЯ

В статье рассмотрена задача с динамическим нелокальным условием для одномерного гиперболического уравнения, возникающая при исследовании колебаний стержня. Эта задача может служить математической моделью процессов, связанных с продольными колебаниями толстого или короткого стержня, и демонстрирует нелокальный подход к изучаемому явлению. Основной результат статьи состоит в обосновании разрешимости поставленной задачи. Получены условия на входные данные, обеспечивающие однозначную разрешимость поставленной задачи, проведено доказательство существования и единственности решения задачи в пространстве Соболева. Доказательство утверждений базируется на полученных в работе априорных оценках, методе Галеркина и свойствах пространств Соболева.

Ключевые слова: гиперболическое уравнение; нелокальная задача; интегральные условия; единственность решения; разрешимость задачи.

Цитирование. Богатов А.В. Задача с динамическим нелокальным условием для одномерного гиперболического уравнения // Вестник Самарского университета. Естественнонаучная серия. 2021. Т. 27, № 1. С. 7–14. DOI: http://doi.org/10.18287/2541-7525-2021-27-1-7-14.

Информация о конфликте интересов: автор и рецензенты заявляют об отсутствии конфликта интересов.

© Богатов А.В., 2021

Андрей Владимирович Богатов — аспирант кафедры дифференциальных уравнений и теории управления, Самарский национальный исследовательский университет имени академика С.П. Королева, 443086, Российская Федерация, г. Самара, Московское шоссе, 34.

Введение

В статье рассмотрена нелокальная задача с интегральным условием, внеинтегральные члены которого содержат как след производной по пространственной переменной, так и след производной по времени, что отражает наличие в рассматриваемой системе демпфера. Такие условия возникают при математическом моделировании многих физических процессов и явлений. Строительные конструкции и сооружения в значительной степени подвержены как природным, так и техногенным динамическим воздействиям, к которым можно отнести ветровые и сейсмические воздействия, нагрузки от оборудования, движущегося транспорта, пешеходов. Энергия колебаний инженерных систем постепенно рассеивается за счет внутреннего трения в материале и внешнего сопротивления, что, безусловно, влияет на их колебательный процесс, а снижение интенсивности внешних динамических воздействий приводит к затуханию колебаний. Для обеспечения безаварийной работы инженерных систем необходимо проводить динамические расчеты конструкций и сооружений, выявлять их динамические характеристики. Также стоит отметить, что необходимо учитывать влияние эффекта внутреннего демпфирования, которое гасит колебания за счет трения в материале и тем самым влияет на общий колебательный процесс. И если уже известно,

как учитывать эффекты внешнего трения (внешнее гашение колебаний), то задача учета внутреннего трения до сих пор не имеет однозначного решения. Переходя к математическим терминам, мы получаем задачу с нелокальными условиями, которая описывает модель внутреннего трения (нелокального демпфирования материала). В современной теории дифференциальных уравнений задачи с нелокальными условиями представляют собой интенсивно развивающееся направление [1–6]. Исследования нелокальных задач показали, что классические подходы к их решению неприменимы [7]. Однако к настоящему времени разработаны некоторые методы, позволяющие преодолеть трудности, возникающие вследствие нелокальных условий [8]. Модификацией одного из них мы и воспользовались для доказательства однозначной разрешимости поставленной задачи в пространстве Соболева.

1. Постановка задачи

В области $Q_T = (0,l) \times (0,T)$ рассмотрим уравнение

$$Lu \equiv u_{tt} - (au_x)_x + bu_t + cu = f(x,t) \tag{1}$$

и поставим задачу: найти решение уравнения (1), удовлетворяющее начальным данным

$$u(x,0) = 0, u_t(x,0) = 0, \tag{2}$$

граничному условию

$$u_x(0,t) = 0 \tag{3}$$

и нелокальному условию

$$u_x(l,t) + \gamma u_t(l,t) + \int_0^l K(x)u_t(x,t)dx = 0. \tag{4}$$

Введем понятие обобщенного решения задачи. Обозначим

$$W(Q_T) = \{u : u \in W_2^1(Q_T), \quad u_t(l,t) \in L_2(0,T)\},$$

$$\hat{W}(Q_T) = \{v : v \in W(Q_T), \ v(x,T) = 0\}.$$

Следуя известной процедуре [9] и предположив, что $u(x,t)$ является классическим решением поставленной задачи, $v(x,t)$ — произвольная гладкая функция, такая, что $v(x,T) = 0$, получим равенство

$$\int_0^T \int_0^l (-u_t v_t + au_x v_x + bu_t v + cuv)dxdt + \int_0^T v(l,t)[\gamma u_t(l,t) + \int_0^l K(x)u_t(x,t)dx]dt$$

$$= \int_0^T \int_0^l f(x,t)v(x,t)dxdt. \tag{5}$$

Заметим, что (5) выполняется, если $u \in W(Q_T), \quad v \in \hat{W}(Q_T)$.

Определение. Обобщенным решением задачи (1)-(4) будем называть функцию $u \in W(Q_T)$, удовлетворяющую условию $u(x,0) = 0$ и тождеству (5) для всех $v \in \hat{W}(Q_T)$.

2. Разрешимость задачи

Теорема 2.1. Если

$$a, a_t, b, b_t, c \in C(\bar{Q}_T), \quad f \in L_2(Q_T), \quad K \in C[0,l], \gamma > 0,$$

то существует единственное обобщенное решение задачи (1)–(4).

Доказательство

Единственность решения. Предположим, что существуют два обобщенных решения $u_1(x,t)$ и $u_2(x,t)$ задачи (1)–(4). Тогда их разность $u(x,t) = u_1(x,t) - u_2(x,t)$ удовлетворяет условию $u(x,0) = 0$ и тождеству

$$\int_0^T \int_0^l (-u_t v_t + au_x v_x + bu_t v + cuv)dxdt + \int_0^T v(l,t)[\gamma u_t(l,t) + \int_0^l Ku_t dx]dt = 0. \tag{6}$$

Выберем в (6)

$$v = \begin{cases} \int_\tau^t u(x,\eta)d\eta, x \leqslant t \leqslant \tau, \\ 0, \tau \leqslant t \leqslant T. \end{cases}$$

Заметим, что $v \in \hat{W}(Q_T)$, причем $v_t(x,t) = u(x,t)$. Интегрируя по частям в левой части (6), в результате несложных преобразований получим

$$\int_0^l [u^2(x,\tau) + av_x^2(x,0)]dx + 2\gamma \int_0^\tau u^2(l,t)dt = 2\int_0^\tau \int_0^l cuvdxdt - \int_0^\tau \int_0^l a_t v_x^2 dxdt -$$

$$- \int_0^\tau \int_0^l bu^2 dxdt - 2\int_0^\tau \int_0^l b_t uvdxdt + 2\int_0^T v(l,t) \int_0^l Ku_t dxdt.$$

Так как по условию $\gamma > 0$, то из этого равенства вытекает неравенство

$$\int_0^l [u^2(x,\tau) + av_x^2(x,0)]dx + 2\gamma \int_0^\tau u(l,t)^2 dt \leqslant 2|\int_0^\tau \int_0^l cuvdxdt| + |\int_0^\tau \int_0^l a_t v_x^2 dxdt| +$$

$$+|\int_0^\tau \int_0^l bu^2 dxdt| + 2|\int_0^\tau \int_0^l b_t uvdxdt| + 2|\int_0^T v(l,t) \int_0^l Ku_t dxdt|. \quad (7)$$

Оценим правую часть (7). Заметим, что в силу условий теоремы существуют числа a_1, c_0, b_0, k_0 такие, что $|a, a_t| \leqslant a_1, |b, b_t| \leqslant b_0, |c| \leqslant c_0, \int_0^l K^2(x)dx \leqslant k_0$. Тогда

$$|\int_0^\tau \int_0^l a_t v_x^2 dxdt| \leqslant a_1 \int_0^\tau \int_0^l v_x^2 dxdt,$$

$$|\int_0^\tau \int_0^l bu^2 dxdt| \leqslant b_0 \int_0^\tau \int_0^l u^2 dxdt.$$

Применяя неравенство Коши, получим

$$2|\int_0^\tau \int_0^l cuvdxdt| \leqslant c_0 \int_0^\tau \int_0^l (u^2 + v^2)dxdt;$$

$$2|\int_0^\tau \int_0^l b_t uvdxdt| \leqslant b_0 \int_0^\tau \int_0^l (u^2 + v^2)dxdt.$$

Прежде чем оценивать последнее слагаемое правой части (7), преобразуем его, интегрируя по частям и учитывая, что $v(x,\tau) = 0$, $u(x,0) = 0$. Получим

$$\int_0^\tau v(l,t) \int_0^l K(x)u_t dxdt = -\int_0^\tau v_t(l,t) \int_0^l K(x)u(x,t)dxdt.$$

Теперь воспользуемся неравенством Коши "с ε" и учтем, что $v_t = u$.

$$|\int_0^\tau u(l,t) \int_0^l K(x)udxdt| \leqslant \varepsilon \int_0^\tau u^2(l,t)dt + c(\varepsilon) \int_0^\tau (\int_0^l Kudx)^2 dt \leqslant$$

$$\leqslant \varepsilon \int_0^\tau u^2(l,t)dt + c(\varepsilon)k_0 \int_0^\tau \int_0^l u^2 dxdt.$$

Выберем ε так, чтобы $2\gamma - \varepsilon > 0$, и перенесем $\varepsilon \int_0^\tau u^2(l,t)dt$ в левую часть. Тогда

$$\int_0^l [u^2(x,\tau) + a_0 v_x^2(x,0)]dx + \nu \int_0^\tau u^2(l,t)dt \leqslant M \int_0^\tau \int_0^l (u^2 + v_x^2)dxdt,$$

где $\nu = 2\gamma - \varepsilon, M = max\{c(\varepsilon)k_0 + a_1; b_0\tau + a_1\}$ и в силу гиперболичности уравнения (1) всюду в $\bar{Q}_T$ $a(x,t) \geqslant a_0 > 0$.

В частности,

$$\int_0^l u^2(x,\tau) + a_0 v_x^2(x,0)dx \leqslant M \int_0^\tau \int_0^l (u^2 + v_x^2)dxdt.$$

Для дальнейшей оценки введем функцию $w(x,t) = \int_0^t u_x d\eta$. Нетрудно видеть, что тогда справедливы равенства

$$v_x(x,t) = w(x,t) - w(x,\tau), \quad v_x(x,0) = -w(x,\tau),$$

что приводит к неравенству

$$\int_0^l [u^2(x,\tau) + a_0 w^2(x,\tau)]dx \leqslant$$

$$\leqslant M \int_0^\tau \int_0^l u^2 dxdt + 2M \int_0^\tau \int_0^l w^2(x,t)dxdt + 2M \int_0^\tau \int_0^l w^2(x,\tau)dxdt. \quad (8)$$

Заметим, что

$$\int_0^\tau \int_0^l w^2(x,\tau)dxdt = \tau \int_0^l w^2(x,\tau)dx.$$

Тогда (8) принимает вид

$$\int_0^l [u^2(x,\tau) + a_0 w^2(x,\tau)]dx \leqslant 2M \int_0^\tau \int_0^l (u^2(x,t) + w^2(x,t))dxdt + 2M\tau \int_0^l w^2(x,\tau)dx.$$

Поскольку τ — произвольно, выберем его так, чтобы $a_0 - 2M\tau \geqslant \frac{a_0}{2}$.

Перенесем $2M\tau \int_0^l w^2(x,\tau)dx$ в левую часть и получим:

$$m_0 \int_0^l [u^2(x,\tau) + w^2(x,\tau)]dx \leqslant 2M \int_0^\tau \int_0^l (u^2(x,t) + w^2(x,t))dxdt,$$

где $m_0 = min\{1, a_0 - 2M\tau\}, \tau \in [0, \frac{a_0}{4M}]$.

Применяя лемму Гронуолла, получим, что $u = 0$ для $\tau \in [0, \frac{a_0}{4M}]$. Теперь рассмотрим следующий промежуток: $\tau \in [\frac{\mu}{4M}, \frac{\mu}{2M}]$. Так же получим $u = 0$. Продолжая эту процедуру так, как описано в [9], приходим к выводу, что $u = 0$ всюду в Q_T. Это и означает, что наше предположение неверно, стало быть, не может существовать более одного обобщенного решения поставленной задачи.

Единственность решения доказана.

Существование решения. Рассмотрим произвольную систему функций $w_k(x)$, принадлежащих $C^2[0,l]$, линейно независимую и полную в $W_2^1(0,l)$.

Будем искать решение в виде $u^m(x,t) = \sum_{k=1}^m c_k(t)w_k(x)$ из соотношений:

$$\int_0^l (u_{tt}^m w_i + a u_x^m w_i^{'} + b u_t^m w_i + c u^m w_i)dx +$$

$$+ w_i(l)[\gamma u_t^m(l,t) + \int_0^l K u_t^m dx] = \int_0^l f w_i dx. \tag{9}$$

Подставив в (9) представление $u^m(x,t)$, приходим к системе обыкновенных дифференциальных уравнений:

$$\sum_{k=1}^m c_k^{''}(t)A_{ik} + c_k^{'}(t)B_{ik}(t) + c_k(t)D_{ik}(t) = g_i(t), \tag{10}$$

где

$$A_{ik} = \int_0^l w_k w_i dx,$$

$$B_{ik}(t) = \int_0^l b(x,t)w_k w_i(l)dx + \gamma w_k(l)w_i(l) + w_i(l)\int_0^l K(x)w_k(x)dx,$$

$$D_{ik}(t) = \int_0^l (a w_k^{'} w_i^{'} + c w_k w_i)dx,$$

$$g_i(t) = \int_0^l f(x,t)w_i(x)dx.$$

присоединив к которой начальные условия

$$c_k(0) = 0, c_k^{'}(0) = 0, \tag{11}$$

получим задачу Коши.

Так как функции $w_k(x)$ линейно независимы, то матрица при старших коэффициентах (10) — матрица Грама, в силу чего система (10) разрешима относительно $c_k^{''}(t)$. Условия теоремы гарантируют ограниченность ее коэффициентов и принадлежность правой части пространству $L_2(0,T)$. Поэтому задача Коши для этой системы однозначно разрешима, причем $c_k'' \in L_1(0,T)$. Таким образом, построена последовательность приближений $\{u^m(x,t)\}$.

Покажем, что из этой последовательности можно выделить подпоследовательность, слабо сходящуюся к элементу пространства $W(Q_T)$.

Для дальнейших шагов в доказательстве существования решения поставленной задачи нам потребуются оценки, к выводу которых мы и перейдем.

Умножим (9) на $c_i^{'}(t)$, просуммируем по i от 1 до m и проинтегрируем в промежутке $[0,\tau]$, получим:

$$\int_0^\tau \int_0^l [u_{tt}^m u_t^m + a u_x^m u_{xt}^m + b(u_t^m)^2 + c u^m u_t^m] dxdt +$$

$$+ \int_0^\tau u_t^m(l,t)[\gamma u_t^m(l,t) + \int_0^l K u_t^m dx] dt = \int_0^\tau \int_0^l f u_t^m dxdt.$$

Интегрируя по частям, приходим к равенству

$$\frac{1}{2}\int_0^l [u_t^m(x,\tau))^2 + a(u_x^m(x,\tau)^2] dx + \gamma \int_0^\tau (u_t^m(l,t))^2 dt =$$

$$= -\int_0^\tau \int_0^l b(u_t^m)^2 dxdt - \int_0^\tau \int_0^l c u^m u_t^m dxdt - \int_0^\tau u_t^m(l,t) \int_0^l K(x) u_t^m(x,t) dxdt +$$

$$+ \frac{1}{2}\int_0^\tau \int_0^l a_t (u_x^m)^2 dxdt + \int_0^\tau \int_0^l f u_t^m dxdt,$$

из которого после умножения обеих частей на 2 следует неравенство

$$\int_0^l [u_t^m(x,\tau))^2 + a(u_x^m(x,\tau)^2] dx + 2\gamma \int_0^\tau (u_t^m(l,t))^2 dt \leqslant$$

$$\leqslant 2\int_0^\tau \int_0^l |b|(u_t^m)^2 dxdt + 2|\int_0^\tau \int_0^l u^m u_t^m dxdt| + 2|\int_0^\tau u_t^m(l,t) \int_0^l K(x) u_t^m(x,t) dxdt| +$$

$$+ \int_0^\tau \int_0^l |a_t|(u_x^m)^2 dxdt + 2|\int_0^\tau \int_0^l f u_t^m dxdt|.$$

Получим априорную оценку, используя технику, продемонстрированную при доказательстве единственности. Особо отметим, что

$$2|\int_0^\tau u_t^m(l,t) \int_0^l K(x) u_t^m(x,t) dxdt| \leqslant$$

$$\leqslant \varepsilon \int_0^\tau (u_t^m(l,t))^2 dt + c(\varepsilon) \int_0^\tau (\int_0^l K u_t^m dx)^2 dt.$$

Выберем ε так, чтобы $2\gamma - \varepsilon > 0$, и перенесем в левую часть первое слагаемое, получим

$$\int_0^l [(u_t^m(x,\tau))^2 + a(u_x^m(x,\tau)^2] dx + \nu \int_0^\tau (u_t^m(l,t))^2 dt \leqslant$$

$$\leqslant 2\int_0^\tau \int_0^l [P(u_t^m)^2 + c_0(u^m)^2 + a_1(u_x^m)^2] dxdt + \int_0^\tau \int_0^l f^2 dxdt,$$

где $P = max\{2b_1 + k_0 + c_0 + 1\}, \nu = 2\gamma - \varepsilon$.

Прибавив к обеим частям очевидное неравенство

$$\int_0^l (u^m(x,\tau))^2 dx \leqslant \tau \int_0^\tau \int_0^l (u_t^m(x,t))^2 dxdt, \tag{12}$$

которое является следствием представления $u^m(x,\tau) = \int_0^\tau u_t^m(x,t) dt$, получим

$$m\int_0^l [(u^m(x,\tau))^2 + (u_t^m(x,\tau))^2 + (u_x^m(x,\tau))^2] dx + \nu \int_0^\tau (u_t^m(l,t))^2 dt \leqslant$$

$$\leqslant P_1 \int_0^\tau \int_0^l [(u^m)^2 + (u_t^m)^2 + (u_x^m)^2] dxdt + \int_0^\tau \int_0^l f^2 dxdt, \tag{13}$$

где $m = min\{1, a_0\}, P_1 = max\{P, c_0, a_1\}$.

В частности,

$$\int_0^l [(u^m(x,\tau))^2 + (u_t^m(x,\tau))^2 + (u_x^m(x,\tau))^2] dx \leqslant$$

$$\leqslant P_2 \int_0^\tau \int_0^l [(u^m)^2 + (u_t^m)^2 + (u_x^m)^2] dxdt + \frac{1}{m}\int_0^\tau \int_0^l f^2 dxdt,$$

где $P_2 = P_1/m$. Применим лемму Гронуолла:

$$\int_0^l [(u^m(x,\tau))^2 + (u_t^m(x,\tau))^2 + (u_x^m(x,\tau))^2]dx \leqslant e^{P_2\tau}\frac{1}{m}||f||^2_{L_2(Q_T)}.$$

После интегрирования по τ в промежутке $[0,T]$:

$$\int_0^T\int_0^l [(u^m(x,\tau))^2 + (u_t^m(x,\tau))^2 + (u_x^m(x,\tau))^2]dxdt \leqslant \frac{1}{P_1}(e^{P_2T}-1)||f||^2_{L_2(Q_T)}.$$

Возвращаясь к (10), рассмотрим и оценим второе слагаемое левой части неравенства:

$$\nu\int_0^\tau (u_t^m(l,t))^2dt \leqslant P_2\int_0^\tau\int_0^l (u^m)^2 + (u_t^m)^2 + (u_x^m)^2dxdt + \int_0^\tau\int_0^l f^2dxdt.$$

Обозначим

$$\frac{1}{P_1}(e^{P_2T}-1) = P_3.$$

Выше было доказано, что

$$\int_0^\tau\int_0^l (u^m)^2 + (u_t^m)^2 + (u_x^m)^2dxdt \leqslant \frac{1}{P_1}(e^{P_2T}-1)||f|| = P_3||f||.$$

Тогда получим

$$\int_0^\tau (u_t^m(l,t))^2dt \leqslant P_4||f||^2, \forall\tau\in[0,T],$$

где $P_4 = P_2P_3 + 1$, откуда получаем, что

$$||u^m(x,t)||^2_{W(Q_T)} \leqslant K, K = max\{P_3, P_4\},$$

причем K не зависит от m. Так как константа в правой части последнего неравенства не зависит от m, то из последовательности $u^m(x,t)$ можно выделить подпоследовательность, слабо сходящуюся к некоторому элементу $u(x,t)\in W(Q_T)$.

Покажем, что этот предел удовлетворяет тождеству (5). Умножим (9) на функцию $h_j(t)\in C^1(Q_T)$, такую, что $h_j(T)=0$, просуммируем по j (от 1 до m) и проинтегрируем по t от 0 до T.

Обозначив

$$\eta(x,t) = \sum_{j=1}^m h_j(t)w_j(x),$$

получаем после интегрирования первого слагаемого левой части

$$\int_0^T\int_0^l (-u_t^m\eta_t + au_x^m\eta_x + bu_t^m\eta + cu^m\eta)dxdt+$$

$$+\int_0^T \eta[\gamma u_t^m(l,t) + \int_0^l Ku_t^m dx]dt = \int_0^T\int_0^l f\eta dxdt. \qquad (14)$$

Тождество (12) справедливо для любой функции $\eta(x,t)$. Обозначим совокупность таких функций $\eta(x,t)$ через σ_m. В (12) перейдем к пределу при фиксированной функции $\eta(x,t)\in\sigma_m$. Это приведет к тождеству (5) для предельной функции $u(x,t)$. Так как совокупность всех функций $\eta(x,t)$ плотна в $W_2^1(Q_T)$ [10], то полученное тождество выполнено для любой функции $v(x,t)\in W_2^1(Q_T)$. Следовательно, $u(x,t)$ — обобщенное решение задачи (1).

Теорема полностью доказана.

Заключение

Таким образом, была поставлена задача с динамическим нелокальным условием для одномерного гиперболического уравнения, возникающая при исследовании колебаний стержня, получено обобщенное решение поставленной задачи. Проведены необходимые преобразования, получены оценки для доказательства единственности и существования решения.

Литература

[1] Гордезиани Д.Г., Авалишвили Г.А. Решения нелокальных задач для одномерных колебаний среды // Матем. моделирование. 2000. Т. 12, № 1. С. 94–103. URL: http://mi.mathnet.ru/mm832

[2] Кожанов А.И. О разрешимости некоторых краевых задач с условием Бицадзе-Самарского для линейных гиперболических уравнений // Современная математика и ее приложения. Тбилиси, 2010. Т. 67. С. 84–96.

[3] Кожанов А.И., Пулькина Л.С. О разрешимости некоторых граничных задач со смещением для линейных гиперболических уравнений // Математический журнал. Алматы. 2009. Т. 9, № 2. С. 78–92.

[4] Пулькина Л.С. О разрешимости в L_2 нелокальной задачи с интегральными условиями для гиперболического уравнения // Дифференциальные уравнения. 2000. Т. 36, № 2. С. 279–280. URL: http://mi.mathnet.ru/de10101.

[5] Пулькина Л.С Смешанная задача с интегральным условием для гиперболического уравнения // Матем. заметки. 2003. Т. 74, № 3. С. 435–445. DOI: https://doi.org/10.4213/mzm277.

[6] Bouziani A. Strong solution to an hyperbolic evolution problem with nonlocal boundary conditions // Maghreb Math. Rev. 2000. V. 9. P. 71–84.

[7] Бейлин С.А. Смешанные задачи с интегральными условиями для волнового уравнения. Самара, 2005.

[8] Pulkina L.S. Solution to nonlocal problems of pseudohyperbolic equations // EJDE. 2014. V. 116. P. 1–9. URL: http://ejde.math.txstate.edu.

[9] Ладыженская О.А. Краевые задачи математической физики. Москва: Наука, 1973. 408 с. URL: https://booksee.org/book/442669.

[10] Михайлов В.П. Дифференциальные уравнения в частных производных. Москва: Наука, 1976. 391 с. URL: https://booksee.org/book/442690.

Scientific article

DOI: 10.18287/2541-7525-2021-27-1-7-14

Submited: 15.01.2021
Revised: 17.02.2021
Accepted: 28.02.2021

A.V. Bogatov
Samara National Research University, Samara, Russian Federation
E-mail: andrebogato@mail.ru. ORCID: https://orcid.org/0000-0001-5797-1930

A PROBLEM WITH NONLOCAL CONDITION FOR ONE-DIMENSIONAL HYPERBOLIC EQUATION

ABSTRACT

In this paper, we study the problem with a dynamic nonlocal condition for the one-dimensional hyperbolic equation, which occurs in the study of rod vibrations. This problem may be used as a mathematical model of longitudinal vibration in a thick short bar and illustrates a nonlocal approach to such processes. Conditions have been obtained for input data, providing unambiguous resolution of the task, proof of the existence and singularity of the problem in the space of Sobolev. The proof is based on the a priori estimates obtained in this paper, Galerkin's procedure and the properties of the Sobolev spaces.

Key words: hyperbolic equation; nonlocal problem; integral conditions; singularity of the solution; solveability of the problem.

Citation. Bogatov A.V. A problem with nonlocal condition for one-dimensional hyperbolic equation. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2021, vol. 27, no. 1, pp. 7–14. DOI: http://doi.org/10.18287/2541-7525-2021-27-1-7-14. (In Russ.)

Information about the conflict of interests: author and reviewers declare no conflict of interests.

© Bogatov A.V., 2021

Andrey Vladimirovich Bogatov — postgraduate student of the Department of Equations of Mathematical Physics, Samara National Research University, 34, Moskovskoye shosse, 443086, Russian Federation.

References

[1] Gordeziani D.G., Avalishvili G.A. On the construcing of solutions of the nonlocal initial boundary value problems for one-dimensional medium oscillation equations. *Mathematical models and Computer Simulations*, 2000, vol. 12, no. 1, pp. 94–103. Available at: http://mi.mathnet.ru/mm832. (In Russ.)

[2] Kozhanov A.I. On the solvability of some boundary value problems with the Bitsadze-Samarsky condition for linear hyperbolic equations. In: *Sovremennaya matematika i ee prilozheniya.* Tbilisi, 2010, vol. 67, pp. 84–96. (In Russ.)

[3] Kozhanov A.I., Pul'kina L.S. On the solvability of some boundary value problems with displacement for linear hyperbolic equations. *Matematicheskii zhurnal*, 2006, no. 42, pp. 1233–1246. (In Russ.)

[4] Pul'kina L.S. The L_2 solvability of a nonlocal problem with integral conditions for a hyperbolic equation. *Differential equations*, 2000, vol. 36, no. 2, pp. 316–318. DOI: https://doi.org/10.1007/BF02754219. (English; Russian original)

[5] Pul'kina L.S. A Mixed Problem with Integral Condition for the Hyperbolic Equation. *Mathematical Notes*, 2003, vol. 74, no. 3, pp. 411–421. DOI: https://doi.org/10.1023/A:1026167021195 (English; Russian original)

[6] Bouziani A. Strong solution to a hyperbolic evolution problem with nonlocal boundary conditions. *Maghreb Math. Rev.*, 2000, vol. 9, pp. 71–84.

[7] Beylin S.A. Mixed problems with integral conditions for the wave equation. Samara, 2005. (In Russ.)

[8] Pulkina L.S. Solution to nonlocal problems of pseudohyperbolic equations. *Electronic Journal of Differential Equations*, 2014, vol. 116, pp. 1–9. Available at: http://ejde.math.txstate.edu.

[9] Ladyzhenskaya O.A. Boundary problems of mathematical physics. Moscow: Nauka, 1973, 407 p. Available at: https://booksee.org/book/442669. (In Russ.)

[10] Mihailov V.P. Partial differential equations. Moscow: Nauka, 1976, 391 p. Available at: https://booksee.org/book/442690. (In Russ.)

Научная статья
DOI: 10.18287/2541-7525-2021-27-1-15–28

УДК 517.956.6

Дата: поступления статьи: 12.01.2021
после рецензирования: 17.02.2021
принятия статьи: 28.02.2021

В.Б. Дмитриев
E-mail: dmitriev_v.b@mail.ru. ORCID: https://orcid.org/0000-0002-9788-7036

КРАЕВАЯ ЗАДАЧА С НЕЛОКАЛЬНЫМ ГРАНИЧНЫМ УСЛОВИЕМ ИНТЕГРАЛЬНОГО ВИДА ДЛЯ МНОГОМЕРНОГО УРАВНЕНИЯ IV ПОРЯДКА

АННОТАЦИЯ

Исследуется разрешимость в классе регулярных (имеющих все обобщенные по С.Л. Соболеву суммируемые с квадратом производные, входящие в соответствующее уравнение) решений нелокальной задачи с интегральным по пространственным переменным условием для линейного уравнения высокого порядка. Обозначается, что вначале подобные задачи изучались для уравнений высокого порядка либо в одномерном случае, либо при выполнении некоторых условий малости на величину T. Также приведен перечень новых работ для многомерного случая. В данной работе приводятся новые результаты о разрешимости нелокальной задачи с интегральными по пространственным переменным условиями для уравнения высокого порядка: а) в многомерном по пространственным переменным случае; б) при отсутствии условий малости на величину T; однако это условие есть на ядро $K(x, y, t)$. Метод исследования основан на получении априорных оценок решения поставленной задачи, из которых следует его существование и единственность в данном пространстве.

Ключевые слова: краевая задача; нелокальное условие; уравнение высокого порядка; априорные оценки; граничные условия интегрального вида; уравнение Буссинеска; регулярные решения; единственность; существование.

Цитирование. Дмитриев В.Б. Краевая задача с нелокальным граничным условием интегрального вида для многомерного уравнения IV порядка // Вестник Самарского университета. Естественнонаучная серия. 2021. Т. 27, № 1. С. 15–28. DOI: http://doi.org/10.18287/2541-7525-2021-27-1-15-28.

Информация о конфликте интересов: автор и рецензенты заявляют об отсутствии конфликта интересов.

© Дмитриев В.Б., 2021
Виктор Борисович Дмитриев — кандидат физико-математических наук.

Введение

Нелокальные задачи с интегральными условиями для дифференциальных уравнений с частными производными в настоящее время весьма активно изучаются, прежде всего для параболических и гиперболических уравнений и для ультрапараболических уравнений; в связи с этим отметим работы [1–5]. Многие постановки задач для них давно стали классическими и вошли в учебники по математической физике.

Отметим, что работы, связанные с исследованием разрешимости нелокальных задач для дифференциальных уравнений в частных производных с граничными условиями интегрального вида, многочисленны. Однако среди них преобладают работы, в которых изучается одномерный по пространственным переменным случай. Важный шаг был сделан в работах А.И. Кожанова и Л.С. Пулькиной [1–3], где была доказана однозначная разрешимости краевых задач с нелокальным граничным условием интегрального вида для многомерных гиперболических уравнений второго порядка.

Многочисленные работы по исследованию уравнений высокого (выше второго) порядка в своем большинстве связаны с изучением классических начальных и начально-краевых задач. Например, математическая модель стержня Рэлея [6], описывающая продольные колебания толстого короткого стержня с учетом поперечного движения стержня; уравнение Кортевега – де Фриза [7], моделирующее процесс распространения длинных волн на поверхности воды; уравнения, описывающие нестационарные волны в стратифицированных и вращающихся жидкостях [8]. В книге «Неклассические уравнения математической физики высокого порядка» [9] приведен обширный перечень работ, посвященных этим вопросам. Примеры явлений, математические модели которых основаны на уравнениях высокого порядка, приведены также в монографии [10].

В работе автора [11] доказана однозначная разрешимость краевой задачи для уравнения высокого порядка в прямоугольнике $Q = \{(x,\tau) : 0 < x < l, 0 < \tau < T\}$, при этом фигурирует производная четвёртого порядка по времени. Однако в этой работе рассмотрен случай одной пространственной переменной и есть ограничения на коэффициенты уравнения. А также есть условия малости как на ядро $K(y)$, фигурирующее в нелокальном условии, так и на величину T.

Отметим здесь также работы Н.С. Попова [12–14], работу А.И. Кожанова и А.В. Дюжевой [15], работы Т.К. Юлдашева [16–18]. В работе [19] для доказательства разрешимости задачи для уравнения четвертого порядка вводится понятие обобщенного решения и доказывается его существование и единственность в выбранном пространстве.

В настоящей работе представлен новый результат о разрешимости нелокальной задачи с граничным условием интегрального вида условиями для уравнения высокого порядка: а) в многомерном по пространственным переменным случае; б) при отсутствии условий малости на величину T; однако это условие есть на ядро $K(x,y,t)$. Притом целью настоящей работы является доказательство существования и единственности регулярного решения — именно решения, имеющего все обобщенные по С.Л. Соболеву производные, входящие в уравнение.

Структурно настоящая работа состоит из четырех частей. В первой из них дается постановка изучаемой задачи. Во второй части приведены основные обозначения и неравенства, используемые в работе, а также сформулирована теорема существования и единственности решения. В третьей и четвертой частях доказываются априорные оценки, с их помощью обосновывается верность теоремы.

1. Постановка задачи

Пусть Ω — ограниченная область пространства $\mathbb{R}^n$ с гладкой (для простоты — бесконечно дифференцируемой) границей Γ, $Q_T = \{(x,\tau) : x \in \Omega \subset \mathbb{R}^n, 0 < \tau < T\}$ - цилиндр конечной высоты T, $S = \Gamma \times (0,T)$ — его боковая граница. Обозначим A_0, A и B — операторы, действие которых на функцию $u(x,t)$ определяется равенствами

$$A_0 u = \sum_{i,j=1}^{n} \frac{\partial}{\partial x_i}\Big(a_{ij}(x,t)\, u_{x_j}\Big), \quad Au = A_0 u + a(x,t)u,$$

$$Bu = \sum_{i,j=1}^{n} \frac{\partial}{\partial x_i}\Big(b_{ij}(x,t)\, u_{x_j}\Big) + b(x,t)u$$

(здесь и далее по повторяющимся индексам ведется суммирование в пределах от 1 до n).

Исследована разрешимость начально-краевой задачи для уравнения высокого порядка

$$L\,u \equiv A_0 u_{tt} + a(x,t)u_{tt} + Bu = f(x,t) \tag{1.1}$$

с эллиптическим оператором A_0 и оператором B произвольного типа с интегральным краевым условием.

Или, более сжато:

$$L\,u \equiv Au_{tt} + Bu = f.$$

Краевая задача: найти функцию $u(x,t)$, являющуюся в цилиндре Q_T решением уравнения

$$L\,u = f(x,t), \tag{1.2}$$

и такую, что для нее выполняются условия:

$$u(x,0) = u_t(x,0) = 0, x \in \Omega, \tag{1.3}$$

$$\frac{\partial u(x,t)}{\partial \nu(x)}|_{(x,t)\in S} \equiv \sum_{i,j=1}^{n} a_{ij}(x,\tau)\, u_{x_j}\, \nu_i|_{(x,t)\in S} = \int\limits_{\Omega} K(x,y,t)\, u(y,t)\, dy|_{(x,t)\in S}. \tag{1.4}$$

Здесь $a_{ij}(x,t), b_{ij}(x,t)(i,j=1,\dots,n), a(x,t), b(x,t), f(x,t)$, и $K(x,y,t)$ — заданные при $x\in\overline{\Omega}, y\in\overline{\Omega}, t\in[0,T]$ функции. Далее, потребуем выполнения условий:

$$a_{ij}(x,t)\xi_i\xi_j \geqslant k_0|\xi|^2, \quad a(x,t)\leqslant -a_0<0,\ \xi\in\mathbb{R}^n,\ x\in\overline{\Omega}, \tag{1.5}$$

$$|K(x,y,t)|\leqslant R_1(y,t), \quad |K_t(x,y,t)|\leqslant R_2(y,t),$$

$$|K_{tt}(x,y,t)|\leqslant R_3(y,t), \quad \forall x,y\in\Omega,\ t\in[0,T]. \tag{1.6}$$

Здесь $k_0>0$, $a_0>0$, — некоторые числа, $R_1(y,t)$, $R_2(y,t)$, $R_3(y,t)$ — заданные при $y\in\overline{\Omega}, t\in[0,T]$ функции.

Заметим, что уравнение (1.2) близко по типу к уравнениям составного типа и, в частности, содержит известное уравнение Буссинеска.

Перейдем к содержательной части работы.

2. Основные обозначения

Пусть $V(Q_T)$ есть следующее пространство функций:

$$V(Q_T)=\Big\{v(x,t): v(x,t)\in L_\infty(0,T;W_2^2(\Omega)),$$

$$v_t(x,t)\in L_\infty(0,T;W_2^2(\Omega)),\ v_{tt}(x,t)\in L_2(0,T;W_2^2(\Omega))\Big\},$$

норму в этом пространстве определим естественным образом:

$$\|v\|_V=\|v\|_{L_2(0,T;W_2^2(\Omega))}+\|v_t\|_{L_\infty(0,T;W_2^2(\Omega))}+\|v_{tt}\|_{L_2(0,T;W_2^2(\Omega))}.$$

Получены условия на функции $a_{ij}(x,t), b_{ij}(x,t), a(x,t), b(x,t), f(x,t)$ и $K(x,y,t)$, при выполнении которых рассматриваемая краевая задача имеет единственное классическое решение из $V(Q_T)$.

При получении априорных оценок решений мы будем использовать элементарное неравенство

$$|ab|\leqslant\frac{a^2+b^2}{2}, \tag{2.1}$$

верное для вещественных a и b, а также "неравенство Коши с δ":

$$2\,|ab|\leqslant\delta a^2+\frac{1}{\delta}b^2. \tag{2.2}$$

Мы также будем использовать неравенство

$$\int\limits_{\partial\Omega}|u|\,ds\leqslant c\int\limits_{\Omega}\Big(|\nabla u|+|u|\Big)\,dx, \tag{2.3}$$

справедливое для любой функции $u\in W_1^1(\Omega)$ и области Ω с гладкой границей [20, с. 77].

Также нам понадобится второе основное неравенство для эллиптических операторов [21]:

$$\sum_{i=1}^n\int\limits_{\Omega}u_{x_i}^2(x,t)\,dx+\sum_{i,j=1}^n\int\limits_{\Omega}u_{x_ix_j}^2(x,t)\,dx\leqslant c_0\|A\,u\|_{L_2(\Omega)}^2+c_1\|u\|_{L_2(\Omega)}^2, \tag{2.4}$$

в котором числа c_0 и c_1 определяются лишь оператором A и областью Ω .

Теорема. Пусть выполняются условия

$$a_{ij}(x,t)\in C^1(Q_T), a_{ij}(x,t)=a_{ji}(x,t), a_{ij}(x,t)\in C^1(\overline{\Omega}),$$

$$b_{ij}(x,t)\in C(\overline{\Omega}), b_i(x,t)\in C(\overline{\Omega}),\ \forall\,t\in[0,T], i,j=1,\dots,n, x\in\overline{\Omega}, \tag{2.5}$$

$$K(x,y,t),\ K_t(x,y,t),\ K_{tt}(x,y,t)\in C(\overline{\Omega}\times\overline{\Omega}\times[0,T]), \tag{2.6}$$

$$R_1(y,t),\ R_2(y,t),\ R_3(y,t)\in L_\infty(0,T;L_2(\Omega)). \tag{2.7}$$

Пусть также выполняются условия (1.5), (1.6) и условия

$$k_0>\frac{1}{2}\,c\,|\Omega|^{\frac{1}{2}}\sup_{t\in[0,T]}\left(\int\limits_{\Omega}R_1^2(y,t)\,dy\right)^{\frac{1}{2}};$$

$$a_0 > \frac{3}{2}\, c\, |\Omega|^{\frac{1}{2}} \sup_{t\in[0,T]} \left(\int\limits_{\Omega} R_1^2(y,t)\, dy \right)^{\frac{1}{2}};$$

$$a(x,t) \in C^1(Q_T),\ b(x,t) \in C(\overline{\Omega}),\ \forall\, t \in [0,T],\ \sup_{t\in[0,T]} \int\limits_{\Omega} |\nabla a(x,t)|^2\, dx < \infty. \tag{2.8}$$

Тогда краевая задача (1.2)–(1.4) имеет решение $u(x,t)$, принадлежащее пространству $V(Q_T)$, и это решение единственно.

3. Доказательство

Доказательство основывается на априорной оценке. Установим ее наличие.

4. Априорная оценка

Умножим уравнение (1.1), записанное в переменных (x,τ), на функцию $-u_\tau(x,\tau)$, результат проинтегрируем по области Q_T и по переменной τ в пределах от 0 до t:

$$-\int\limits_0^t \int\limits_{\Omega} A\, u_{\tau\tau} u_\tau\, dx\, d\tau = \int\limits_0^t \int\limits_{\Omega} B\, u\, u_\tau\, dx\, d\tau - \int\limits_0^t \int\limits_{\Omega} f\, u_\tau\, dx\, d\tau.$$

$$-\int\limits_0^t \int\limits_{\Omega} \sum_{i,j=1}^n a_{ij}(x,\tau)\, (u_{x_i\tau} u_{x_j\tau})_\tau\, dx\, d\tau =$$

$$= -\int\limits_{\Omega} \sum_{i,j=1}^n a_{ij}(x,\tau)\, (u_{x_i\tau} u_{x_j\tau})|_{\tau=0}^{\tau=t}\, dx + \int\limits_0^t \int\limits_{\Omega} \sum_{i,j=1}^n a_{ij\tau}(x,\tau)\, u_{x_i\tau} u_{x_j\tau}\, dx\, d\tau.$$

$$\frac{1}{2} \int\limits_0^t \int\limits_{\Omega} a(x,\tau)\, (u_\tau^2)_\tau\, dx\, d\tau = \frac{1}{2} \int\limits_{\Omega} a(x,\tau)\, u_\tau^2|_{\tau=0}^{\tau=t}\, dx - \frac{1}{2} \int\limits_0^t \int\limits_{\Omega} a_\tau(x,\tau)\, u_\tau^2\, dx\, d\tau.$$

Интегрируя по частям и используя условие (1.4), нетрудно получить следующее неравенство:

$$\int\limits_{\Omega} \sum_{i,j=1}^n a_{ij}(x,\tau)\, (u_{x_i\tau} u_{x_j\tau})|_{\tau=0}^{\tau=t}\, dx - \int\limits_0^t \int\limits_{\Omega} \sum_{i,j=1}^n a_{ij\tau}(x,\tau)\, u_{x_i\tau} u_{x_j\tau}\, dx\, d\tau -$$

$$-\frac{1}{2} \int\limits_{\Omega} a(x,\tau)\, u_\tau^2|_{\tau=0}^{\tau=t}\, dx + \frac{1}{2} \int\limits_0^t \int\limits_{\Omega} a_\tau(x,\tau)\, u_\tau^2\, dx\, d\tau -$$

$$-\int\limits_0^t \int\limits_{\partial\Omega} u_\tau \left(\int\limits_{\Omega} K(x,y,\tau)\, u(y,\tau)\, dy \right)_{\tau\tau} ds\, d\tau -$$

$$-\int\limits_0^t \int\limits_{\Omega} \sum_{i,j=1}^n \frac{\partial}{\partial x_i} \Big(b_{ij}(x,t)\, u_{x_j} \Big) u_\tau\, dx\, d\tau -$$

$$-\frac{1}{2} \int\limits_0^t \int\limits_{\Omega} b(x,\tau)\, (u^2)_\tau\, dx\, d\tau =$$

$$= \int\limits_0^t \int\limits_{\Omega} f(x,\tau)\, u_\tau\, dx\, d\tau.$$

Обозначим

$$I_1 = \int\limits_0^t \int\limits_{\partial\Omega} u_\tau \left(\int\limits_{\Omega} K(x,y,\tau)\, u(y,\tau)\, dy \right)_{\tau\tau} ds\, d\tau,$$

$$I_2 = \int\limits_0^t \int\limits_{\partial\Omega} u_{\tau\tau} \left(\int\limits_{\Omega} K(x,y,\tau)\, u(y,\tau)\, dy \right)_{\tau\tau} ds\, d\tau.$$

Получаем

$$I_1 = \int\limits_0^t \int\limits_{\partial\Omega} u_\tau \int\limits_{\Omega} \Big(K_{\tau\tau}(x,y,\tau)\, u(y,\tau) + 2\, K_\tau(x,y,\tau)\, u_\tau(y,\tau) +$$
$$+ K(x,y,\tau)\, u_{\tau\tau}(y,\tau) \Big)\, dy\, ds\, d\tau.$$

Далее, это слагаемое оценим следующим образом, используя неравенство (2.3):

$$|I_1| \leqslant \int\limits_0^t \int\limits_{\partial\Omega} |u_\tau| \int\limits_{\Omega} \Big(R_3(y,\tau)\, |u(y,\tau)| + 2\, R_2(y,\tau)\, |u_\tau(y,\tau)| +$$
$$+ R_1(y,\tau)\, |u_{\tau\tau}(y,\tau)| \Big)\, dy\, ds\, d\tau \leqslant$$

$$\leqslant c \int\limits_0^t \int\limits_{\Omega} \Big(|u_\tau| + |\nabla u_\tau| \Big) \int\limits_{\Omega} \Big(R_3(y,\tau)\, |u(y,\tau)| + 2\, R_2(y,\tau)\, |u_\tau(y,\tau)| +$$
$$+ R_1(y,\tau)\, |u_{\tau\tau}(y,\tau)| \Big)\, dy\, dx\, d\tau.$$

Аналогично оценим слагаемое I_2, которое у нас появится ниже:

$$|I_2| \leqslant c \int\limits_0^t \int\limits_{\Omega} \Big(|u_{\tau\tau}| + |\nabla u_{\tau\tau}| \Big) \int\limits_{\Omega} \Big(R_3(y,\tau)\, |u(y,\tau)| + 2\, R_2(y,\tau)\, |u_\tau(y,\tau)| +$$
$$+ R_1(y,\tau)\, |u_{\tau\tau}(y,\tau)| \Big)\, dy\, dx\, d\tau.$$

Обозначим

$$z_1(t) = \int\limits_{\Omega} \sum_{i,j=1}^n a_{ij}(x,\tau)\, (u_{x_i\tau} u_{x_j\tau})|_{\tau=t}\, dx - \frac{1}{2} \int\limits_{\Omega} a(x,\tau)\, u_\tau^2|_{\tau=t}\, dx \geqslant$$
$$\geqslant k_0 \sum_{i=1}^n \int\limits_{\Omega} u_{x_i t}^2(x,t)\, dx + \frac{a_0}{2} \int\limits_{\Omega} u_t^2(x,t)\, dx.$$

После оценок получаем

$$z_1(t) \leqslant z_1(0) + \left| \int\limits_0^t \int\limits_{\Omega} \sum_{i,j=1}^n a_{ij\tau}(x,\tau)\, u_{x_i\tau} u_{x_j\tau}\, dx\, d\tau \right| +$$
$$+ c \int\limits_0^t \int\limits_{\Omega} \Big(|u_\tau| + |\nabla u_\tau| \Big) \int\limits_{\Omega} \Bigg(R_3(y,\tau)\, |u(y,\tau)| + 2\, R_2(y,\tau)\, |u_\tau(y,\tau)| +$$
$$+ R_1(y,\tau)\, |u_{\tau\tau}(y,\tau)| \Bigg)\, dy\, dx\, d\tau +$$
$$+ \frac{1}{2} \left| \int\limits_0^t \int\limits_{\Omega} a_\tau(x,\tau)\, u_\tau^2\, dx\, d\tau \right| + \left| \int\limits_0^t \int\limits_{\Omega} \sum_{i,j=1}^n \frac{\partial}{\partial x_i} \Big(b_{ij}(x,\tau)\, u_{x_j} \Big) u_\tau\, dx\, d\tau \right| +$$
$$+ \left| \int\limits_0^t \int\limits_{\Omega} b(x,\tau)\, u\, u_\tau\, dx\, d\tau \right| + \left| \int\limits_0^t \int\limits_{\Omega} f(x,\tau)\, u_\tau\, dx\, d\tau \right|. \tag{4.1}$$

Используя неравенства (2.1), (2.2), а также условия (1.5), (1.6), (2.5)–(2.8), получаем

$$z_1(t) \leqslant z_1(0) + \delta_1^2 \int\limits_0^t \int\limits_{\Omega} u_{\tau\tau}^2(x,\tau)\, dx\, d\tau + P_1 \Big(\sum_{i,j=1}^n \int\limits_0^t \int\limits_{\Omega} u_{x_i x_j}^2(x,\tau)\, dx\, d\tau +$$

$$+\int\limits_0^t\int\limits_\Omega |\nabla u_\tau(x,\tau)|^2\,dx\,d\tau+\int\limits_0^t\int\limits_\Omega u_\tau^2(x,\tau)\,dx\,d\tau+$$

$$+\int\limits_0^t\int\limits_\Omega u^2(x,\tau)\,dx\,d\tau+\int\limits_0^t\int\limits_\Omega f^2(x,\tau)\,dx\,d\tau\Big), \tag{4.2}$$

где число δ_1 — произвольное положительное число, P_1 есть число, определяющееся коэффициентами оператора B, а также областью Q_T и числом δ_1.

Умножим уравнение (1.1), записанное в переменных (x,τ), на функцию $-u_{\tau\tau}(x,\tau)$, результат проинтегрируем по области Q_T и по переменной τ в пределах от 0 до t:

$$-\int\limits_0^t\int\limits_\Omega A\,u_{\tau\tau}u_{\tau\tau}\,dx\,d\tau=\int\limits_0^t\int\limits_\Omega B\,u\,u_{\tau\tau}\,dx\,d\tau-\int\limits_0^t\int\limits_\Omega f\,u_{\tau\tau}\,dx\,d\tau.$$

Интегрируя по частям, получаем следующее равенство:

$$-\int\limits_0^t\int\limits_\Omega\sum_{i,j=1}^n a_{ij}(x,\tau)\,u_{x_i\tau\tau}u_{x_j\tau\tau}\,dx\,d\tau+$$

$$+\int\limits_0^t\int\limits_{\partial\Omega} u_{\tau\tau}\left(\int\limits_\Omega K(x,y,\tau)\,u(y,\tau)\,dy\right)_{\tau\tau}ds\,d\tau-$$

$$-\int\limits_0^t\int\limits_\Omega a(x,\tau)\,u_{\tau\tau}^2\,dx\,d\tau-\int\limits_0^t\int\limits_\Omega B\,u\,u_{\tau\tau}\,dx\,d\tau=-\int\limits_0^t\int\limits_\Omega f\,u_{\tau\tau}\,dx\,d\tau.$$

Здесь появляется слагаемое I_2, которое мы оценили выше. При этом основную трудность представляет слагаемое, содержащее множитель $R_1(y,\tau)$, которое оценим в итоге следующим образом, используя неравенство Коши — Буняковского, а также элементарное неравенство (2.1):

$$c\int\limits_0^t\int\limits_\Omega\Big(|u_{\tau\tau}|+|\nabla u_{\tau\tau}|\Big)\int\limits_\Omega\Big(R_1(y,\tau)\,|u_{\tau\tau}(y,\tau)|\Big)\,dy\,dx\,d\tau$$

$$\leqslant c\int\limits_0^t\int\limits_\Omega\Big(|u_{\tau\tau}|+|\nabla u_{\tau\tau}|\Big)\left(\int\limits_\Omega R_1^2(y,\tau)\,dy\cdot\int\limits_\Omega|u_{\tau\tau}^2(y,\tau)|\,dy\right)^{\frac12}dx\,d\tau\leqslant$$

$$\leqslant c\sup_{\tau\in[0,T]}\left(\int\limits_\Omega R_1^2(y,\tau)\,dy\right)^{\frac12}\int\limits_0^t\left(\int\limits_\Omega|u_{\tau\tau}^2(y,\tau)|\,dy\right)^{\frac12}\int\limits_\Omega\Big(|u_{\tau\tau}|+|\nabla u_{\tau\tau}|\Big)\,dx\,d\tau\leqslant$$

$$\leqslant c\,|\Omega|^{\frac12}\sup_{\tau\in[0,T]}\left(\int\limits_\Omega R_1^2(y,\tau)\,dy\right)^{\frac12}\int\limits_0^t\left(\int\limits_\Omega|u_{\tau\tau}^2(y,\tau)|\,dy\right)^{\frac12}\times$$

$$\times\left\{\left(\int\limits_\Omega|u_{\tau\tau}|^2\,dx\,d\tau\right)^{\frac12}+\left(\int\limits_\Omega|\nabla u_{\tau\tau}|^2\,dx\,d\tau\right)^{\frac12}\right\}\leqslant$$

$$\leqslant c\,|\Omega|^{\frac12}\sup_{\tau\in[0,T]}\left(\int\limits_\Omega R_1^2(y,\tau)\,dy\right)^{\frac12}\times$$

$$\times\left\{\frac12\sum_{i=1}^n\int\limits_0^t\int\limits_\Omega u_{x_i\tau\tau}^2(x,\tau)\,dx\,d\tau+\frac32\int\limits_0^t\int\limits_\Omega u_{\tau\tau}^2(x,\tau)\,dx\,d\tau\right\}.$$

Обозначим

$$z_2(t) = \int\limits_0^t \int\limits_\Omega \sum_{i,j=1}^n a_{ij}(x,\tau)\, u_{x_i\tau\tau} u_{x_j\tau\tau}\, dx\, d\tau - \int\limits_0^t \int\limits_\Omega a(x,\tau)\, u_{\tau\tau}^2\, dx\, d\tau \geqslant$$

$$\geqslant k_0 \sum_{i=1}^n \int\limits_0^t \int\limits_\Omega u_{x_i\tau\tau}^2(x,\tau)\, dx\, d\tau + a_0 \int\limits_0^t \int\limits_\Omega u_{\tau\tau}^2(x,\tau)\, dx\, d\tau.$$

После оценок получаем, используя неравенства (2.1), (2.2), а также условия (1.5), (1.6), (2.5)–(2.8), с учетом того, что $z_2(0) = 0$:

$$z_2(t) \leqslant \left| \int\limits_0^t \int\limits_\Omega B\, u\, u_{\tau\tau}\, dx\, d\tau \right| + \left| \int\limits_0^t \int\limits_\Omega f\, u_{\tau\tau}\, dx\, d\tau \right| +$$

$$+c \int\limits_0^t \int\limits_\Omega \Big(|u_{\tau\tau}| + |\nabla u_{\tau\tau}| \Big) \int\limits_\Omega \Big(R_3(y,\tau)\, |u(y,\tau)| +$$

$$+2\, R_2(y,\tau)\, |u_\tau(y,\tau)| \Big)\, dy\, dx\, d\tau + c\, |\Omega|^{\frac{1}{2}} \sup_{\tau\in[0,T]} \left(\int\limits_\Omega R_1^2(y,\tau)\, dy \right)^{\frac{1}{2}} \times$$

$$\times \left\{ \frac{1}{2} \sum_{i=1}^n \int\limits_0^t \int\limits_\Omega u_{x_i\tau\tau}^2(x,\tau)\, dx\, d\tau + \frac{3}{2} \int\limits_0^t \int\limits_\Omega u_{\tau\tau}^2(x,\tau)\, dx\, d\tau \right\} \leqslant$$

$$\leqslant \delta_2^2 \int\limits_0^t \int\limits_\Omega u_{\tau\tau}^2(x,\tau)\, dx\, d\tau +$$

$$+P_2 \Big(\sum_{i,j=1}^n \int\limits_0^t \int\limits_\Omega u_{x_ix_j}^2(x,\tau)\, dx\, d\tau + \int\limits_0^t \int\limits_\Omega |\nabla u_\tau(x,\tau)|^2\, dx\, d\tau +$$

$$+ \int\limits_0^t \int\limits_\Omega u_\tau^2(x,\tau)\, dx\, d\tau + \int\limits_0^t \int\limits_\Omega u^2(x,\tau)\, dx\, d\tau + \int\limits_0^t \int\limits_\Omega f^2(x,\tau)\, dx\, d\tau \Big) +$$

$$+c\, |\Omega|^{\frac{1}{2}} \sup_{\tau\in[0,T]} \left(\int\limits_\Omega R_1^2(y,\tau)\, dy \right)^{\frac{1}{2}} \times$$

$$\times \left\{ \frac{1}{2} \sum_{i=1}^n \int\limits_0^t \int\limits_\Omega u_{x_i\tau\tau}^2(x,\tau)\, dx\, d\tau + \frac{3}{2} \int\limits_0^t \int\limits_\Omega u_{\tau\tau}^2(x,\tau)\, dx\, d\tau \right\}. \tag{4.3}$$

Теперь для получения оценок умножим уравнение (1.1), записанное в переменных (x,τ), на $A_0\, u_\tau(x,\tau)$, интегрируя, имеем

$$\frac{1}{2} \int\limits_0^t \int\limits_\Omega (A_0\, u_\tau)_\tau^2\, dx\, d\tau - \int\limits_0^t \int\limits_\Omega \sum_{i,j=1}^n \frac{\partial}{\partial x_i} \Big(a_{ij\tau}(x,t)\, u_{x_j\tau} \Big) A_0\, u_\tau\, dx\, d\tau +$$

$$+ \int\limits_0^t \int\limits_\Omega a(x,\tau)\, u_{\tau\tau} A_0\, u_\tau\, dx\, d\tau + \int\limits_0^t \int\limits_\Omega B\, u\, A_0\, u_\tau\, dx\, d\tau = \int\limits_0^t \int\limits_\Omega f\, A_0\, u_\tau\, dx\, d\tau$$

и далее, вводя обозначение $z_3(t) = \int\limits_\Omega (A_0 u_t(x,t))^2 dx$, используя неравенства (2.1), (2.2), а также условия (1.5), (1.6), (2.5)–(2.8), получаем

$$z_3(t) \leqslant z_3(0) + \delta_3^2 \int\limits_0^t \int\limits_\Omega u_{\tau\tau}^2(x,\tau)\, dx\, d\tau + P_3 \Bigg(\int\limits_0^t \int\limits_\Omega (A_0 u_\tau(x,\tau))^2 dx\, d\tau +$$

$$+\sum_{i,j=1}^{n}\int_0^t\int_\Omega u^2_{x_ix_j}(x,\tau)\,dx\,d\tau+\int_0^t\int_\Omega|\nabla u_\tau(x,\tau)|^2\,dx\,d\tau+$$

$$+\int_0^t\int_\Omega u^2_\tau(x,\tau)\,dx\,d\tau+\int_0^t\int_\Omega u^2(x,\tau)\,dx\,d\tau+\int_0^t\int_\Omega f^2(x,\tau)\,dx\,d\tau\Bigg). \tag{4.4}$$

Складывая (4.2)–(4.4), получаем для величины $p(t)=z_1(t)+z_2(t)+z_3(t)$ следующую оценку:

$$p(t)\leqslant p(0)+\left(\delta_1^2+\delta_2^2+\delta_3^2\right)\int_0^t\int_\Omega u^2_{\tau\tau}(x,\tau)\,dx\,d\tau+$$

$$+P_4\Big(\sum_{i,j=1}^{n}\int_0^t\int_\Omega u^2_{x_ix_j}(x,\tau)\,dx\,d\tau+\int_0^t\int_\Omega|\nabla u_\tau(x,\tau)|^2\,dx\,d\tau+$$

$$+\int_0^t\int_\Omega u^2_\tau(x,\tau)\,dx\,d\tau+\int_0^t\int_\Omega u^2(x,\tau)\,dx\,d\tau+\int_0^t\int_\Omega f^2(x,\tau)\,dx\,d\tau\Big)+$$

$$+c\,|\Omega|^{\frac12}\sup_{\tau\in[0,T]}\left(\int_\Omega R_1^2(y,\tau)\,dy\right)^{\frac12}\times$$

$$\times\left\{\frac12\sum_{i=1}^{n}\int_0^t\int_\Omega u^2_{x_i\tau\tau}(x,\tau)\,dx\,d\tau+\frac32\int_0^t\int_\Omega u^2_{\tau\tau}(x,\tau)\,dx\,d\tau\right\}. \tag{4.5}$$

Число P_4 определяется числами P_1, P_2 и P_3. Далее, выписывая выражение в определении $p(t)$, получаем

$$\int_\Omega\sum_{i,j=1}^{n}a_{ij}(x,\tau)\,(u_{x_i\tau}u_{x_j\tau})|_{\tau=t}\,dx-\frac12\int_\Omega a(x,\tau)\,u^2_\tau|_{\tau=t}\,dx+$$

$$+\int_0^t\int_\Omega\sum_{i,j=1}^{n}a_{ij}(x,\tau)\,u_{x_i\tau\tau}u_{x_j\tau\tau}\,dx\,d\tau-\int_0^t\int_\Omega a(x,\tau)\,u^2_{\tau\tau}\,dx\,d\tau+\int_\Omega(A_0u_t(x,t))^2dx\leqslant$$

$$\leqslant p(0)+\left(\delta_1^2+\delta_2^2+\delta_3^2\right)\int_0^t\int_\Omega u^2_{\tau\tau}(x,\tau)\,dx\,d\tau+$$

$$+P_4\Big(\sum_{i,j=1}^{n}\int_0^t\int_\Omega u^2_{x_ix_j}(x,\tau)\,dx\,d\tau+\int_0^t\int_\Omega|\nabla u_\tau(x,\tau)|^2\,dx\,d\tau+$$

$$+\int_0^t\int_\Omega u^2_\tau(x,\tau)\,dx\,d\tau+\int_0^t\int_\Omega u^2(x,\tau)\,dx\,d\tau+\int_0^t\int_\Omega f^2(x,\tau)\,dx\,d\tau\Big)+$$

$$+c\,|\Omega|^{\frac12}\sup_{\tau\in[0,T]}\left(\int_\Omega R_1^2(y,\tau)\,dy\right)^{\frac12}\times$$

$$\times\left\{\frac12\sum_{i=1}^{n}\int_0^t\int_\Omega u^2_{x_i\tau\tau}(x,\tau)\,dx\,d\tau+\frac32\int_0^t\int_\Omega u^2_{\tau\tau}(x,\tau)\,dx\,d\tau\right\}. \tag{4.6}$$

Теперь, учитывая оценки для $z_1(t),z_2(t),z_3(t)$ и приводя подобные слагаемые, получаем

$$k_0\sum_{i=1}^{n}\int_\Omega u^2_{x_it}(x,t)\,dx+\frac{a_0}{2}\int_\Omega u^2_t(x,t)\,dx+\int_\Omega(A_0u_t(x,t))^2dx+$$

$$+\left(k_0-\frac{1}{2}\,c\,|\Omega|^{\frac{1}{2}}\sup_{\tau\in[0,T]}\left(\int\limits_{\Omega}R_1^2(y,\tau)\,dy\right)^{\frac{1}{2}}\right)\sum_{i=1}^{n}\int\limits_0^t\int\limits_{\Omega}u_{x_i\tau\tau}^2(x,\tau)\,dx\,d\tau+$$

$$+\left(a_0-\frac{3}{2}\,c\,|\Omega|^{\frac{1}{2}}\sup_{\tau\in[0,T]}\left(\int\limits_{\Omega}R_1^2(y,\tau)\,dy\right)^{\frac{1}{2}}-\delta_1^2-\delta_2^2-\delta_3^2\right)\int\limits_0^t\int\limits_{\Omega}u_{\tau\tau}^2(x,\tau)\,dx\,d\tau\leqslant$$

$$\leqslant p(0)+P_4\Big(\sum_{i,j=1}^{n}\int\limits_0^t\int\limits_{\Omega}u_{x_ix_j}^2(x,\tau)\,dx\,d\tau+\int\limits_0^t\int\limits_{\Omega}|\nabla u_\tau(x,\tau)|^2\,dx\,d\tau+$$

$$+\int\limits_0^t\int\limits_{\Omega}u_\tau^2(x,\tau)\,dx\,d\tau+\int\limits_0^t\int\limits_{\Omega}u^2(x,\tau)\,dx\,d\tau+\int\limits_0^t\int\limits_{\Omega}f^2(x,\tau)\,dx\,d\tau\Big).\qquad(4.7)$$

В силу условий теоремы и произвольности чисел δ_1, δ_2, δ_3 мы можем выбрать их так, чтобы все коэффициенты в левой части были положительны, то есть чтобы выполнялось неравенство

$$a_0-\frac{3}{2}\,c\,|\Omega|^{\frac{1}{2}}\sup_{\tau\in[0,T]}\left(\int\limits_{\Omega}R_1^2(y,\tau)\,dy\right)^{\frac{1}{2}}-\delta_1^2-\delta_2^2-\delta_3^2>0.$$

Имеют место представления

$$u(x,\tau)=\int\limits_0^{\tau}u_\xi(x,\xi)d\xi=\int\limits_0^{\tau}\int\limits_0^{\xi}u_{\nu\nu}(x,\nu)d\nu\,d\xi.$$

$$u_{x_i}(x,\tau)=\int\limits_0^{\tau}u_{x_i\xi}(x,\xi)d\xi=\int\limits_0^{\tau}\int\limits_0^{\xi}u_{x_i\nu\nu}(x,\nu)d\nu\,d\xi.$$

$$u_{x_ix_j}(x,\tau)=\int\limits_0^{\tau}u_{x_ix_j\xi}(x,\xi)d\xi=\int\limits_0^{\tau}\int\limits_0^{\xi}u_{x_ix_j\nu\nu}(x,\nu)d\nu\,d\xi.$$

Из этих равенств, вновь из второго основного неравенства для эллиптических операторов и леммы Гронуолла [22, с. 23], следует оценка

$$\sum_{i=1}^{n}\int\limits_{\Omega}u_{x_it}^2(x,t)\,dx+\int\limits_{\Omega}u_t^2(x,t)\,dx+\int\limits_{\Omega}(A_0u_t(x,t))^2dx+$$

$$+\sum_{i=1}^{n}\int\limits_0^t\int\limits_{\Omega}u_{x_i\tau\tau}^2(x,\tau)\,dx\,d\tau+\int\limits_0^t\int\limits_{\Omega}u_{\tau\tau}^2(x,\tau)\,dx\,d\tau\leqslant K_0\,\|f\|_{L_2(Q_T)}.\qquad(4.8)$$

Теперь умножим уравнение (1.1), записанное в переменных (x,τ), на $A_0\,u_{\tau\tau}(x,\tau)$, имеем

$$\int\limits_0^t\int\limits_{\Omega}(A_0\,u_{\tau\tau})^2\,dx\,d\tau+\int\limits_0^t\int\limits_{\Omega}a(x,\tau)\,u_{\tau\tau}A_0\,u_{\tau\tau}\,dx\,d\tau+\int\limits_0^t\int\limits_{\Omega}B\,u\,A_0\,u_{\tau\tau}\,dx\,d\tau=$$

$$=\int\limits_0^t\int\limits_{\Omega}f\,A_0\,u_{\tau\tau}\,dx\,d\tau.$$

Обозначим второе слагаемое в левой части через J_1 и преобразуем его:

$$J_1=\int\limits_0^t\int\limits_{\Omega}a(x,\tau)\,u_{\tau\tau}\,A_0\,u_{\tau\tau}dx\,d\tau=\int\limits_0^t\int\limits_{\Omega}a(x,\tau)\,u_{\tau\tau}\sum_{i,j=1}^{n}\left(a_{ij}(x,\tau)\,u_{x_j\tau\tau}\right)_{x_i}dx\,d\tau=$$

$$=\int\limits_0^t\int\limits_{\partial\Omega}\sum_{i,j=1}^{n}a_{ij}(x,\tau)\,u_{x_j\tau\tau}\nu_i\cdot a(x,\tau)\,u_{\tau\tau}\,ds\,d\tau-$$

$$-\int\limits_0^t \int\limits_\Omega \sum_{i,j=1}^n a_{ij}(x,\tau)\, u_{x_j\tau\tau} \Big\{ a(x,\tau)\, u_{\tau\tau} \Big\}_{x_i} dx\, d\tau =$$

$$= \int\limits_0^t \int\limits_{\partial\Omega} a(x,\tau)\, u_{\tau\tau} \left(\int\limits_\Omega K(x,y,\tau)\, u(y,\tau)\, dy \right)_{\tau\tau} ds\, d\tau -$$

$$-\int\limits_0^t \int\limits_\Omega a(x,\tau) \sum_{i,j=1}^n a_{ij}(x,\tau)\, u_{x_j\tau\tau}\, u_{x_i\tau\tau}\, dx\, d\tau.$$

$$-\int\limits_0^t \int\limits_\Omega u_{\tau\tau} \sum_{i,j=1}^n a_{ij}(x,\tau)\, a_{x_i}(x,\tau)\, u_{x_j\tau\tau}\, dx\, d\tau.$$

Далее, оцениваем:

$$\left| \int\limits_0^t \int\limits_{\partial\Omega} a(x,\tau)\, u_{\tau\tau} \left(\int\limits_\Omega K(x,y,\tau)\, u(y,\tau)\, dy \right)_{\tau\tau} ds\, d\tau \right| \leqslant$$

$$\leqslant c \int\limits_0^t \int\limits_\Omega \Big(|a(x,\tau)\, u_{\tau\tau}| + |a(x,\tau)\, \nabla u_{\tau\tau}| + |u_{\tau\tau}\, \nabla a(x,\tau)| \Big) \times$$

$$\times \int\limits_\Omega \Big(R_3(y,\tau)\, |u(y,\tau)| + 2\, R_2(y,\tau)\, |u_\tau(y,\tau)| +$$

$$+ R_1(y,\tau)\, |u_{\tau\tau}(y,\tau)| \Big)\, dy\, ds\, d\tau.$$

Заметим, что из условий (2.8) следует, что

$$\int\limits_\Omega |a(x,t)|^2\, dx < G, \quad \int\limits_\Omega |\nabla a(x,t)|^2\, dx < G \quad \forall t \in [0,T]$$

для некоторого числа G. Как уже было сказано выше, основную трудность представляет слагаемое, содержащее множитель $R_1(y,\tau)$, которое оценим в итоге следующим образом, используя неравенство Коши — Буняковского, а также элементарное неравенство (2.1):

$$c \int\limits_0^t \int\limits_\Omega \Big(|a(x,\tau)\, u_{\tau\tau}| + |a(x,\tau)\, \nabla u_{\tau\tau}| + |u_{\tau\tau}\, \nabla a(x,\tau)| \Big) \int\limits_\Omega \Big(R_1(y,\tau)\, |u_{\tau\tau}(y,\tau)| \Big)\, dy\, dx\, d\tau \leqslant$$

$$\leqslant c \int\limits_0^t \int\limits_\Omega \Big(|a(x,\tau)\, u_{\tau\tau}| + |a(x,\tau)\, \nabla u_{\tau\tau}| + |u_{\tau\tau}\, \nabla a(x,\tau)| \Big) \Big(\int\limits_\Omega R_1^2(y,\tau)\, dy \times$$

$$\times \int\limits_\Omega |u_{\tau\tau}^2(y,\tau)|\, dy \Big)^{\frac{1}{2}} dx\, d\tau \leqslant c \sup_{\tau\in[0,T]} \left(\int\limits_\Omega R_1^2(y,\tau)\, dy \right)^{\frac{1}{2}} \int\limits_0^t \left(\int\limits_\Omega |u_{\tau\tau}^2(y,\tau)|\, dy \right)^{\frac{1}{2}} \times$$

$$\times \int\limits_\Omega \Big(|a(x,\tau)\, u_{\tau\tau}| + |a(x,\tau)\, \nabla u_{\tau\tau}| + |u_{\tau\tau}\, \nabla a(x,\tau)| \Big)\, dx\, d\tau \leqslant$$

$$\leqslant c \sup_{\tau\in[0,T]} \left(\int\limits_\Omega R_1^2(y,\tau)\, dy \right)^{\frac{1}{2}} \int\limits_0^t \left(\int\limits_\Omega |u_{\tau\tau}^2(y,\tau)|\, dy \right)^{\frac{1}{2}} \times$$

$$\times \Bigg\{ \left(\int\limits_\Omega |a(x,\tau)|^2\, dx \right)^{\frac{1}{2}} \left(\int\limits_\Omega |u_{\tau\tau}|^2\, dx \right)^{\frac{1}{2}} + \left(\int\limits_\Omega |\nabla a(x,\tau)|^2\, dx \right)^{\frac{1}{2}} \left(\int\limits_\Omega |u_{\tau\tau}|^2\, dx \right)^{\frac{1}{2}} +$$

$$+ \left(\int\limits_\Omega |a(x,\tau)|^2\, dx \right)^{\frac{1}{2}} \left(\int\limits_\Omega |\nabla u_{\tau\tau}|^2\, dx \right)^{\frac{1}{2}} \Bigg\}\, d\tau \leqslant c\, G^{\frac{1}{2}} \sup_{\tau\in[0,T]} \left(\int\limits_\Omega R_1^2(y,\tau)\, dy \right)^{\frac{1}{2}} \times$$

$$\times \left\{ \frac{1}{2} \sum_{i=1}^{n} \int_0^t \int_\Omega u^2_{x_i\tau\tau}(x,\tau)\, dx\, d\tau + \frac{5}{2} \int_0^t \int_\Omega u^2_{\tau\tau}(x,\tau)\, dx\, d\tau \right\}.$$

Тогда имеем:

$$\int_0^t \int_\Omega (A_0\, u_{\tau\tau})^2\, dx\, d\tau - \int_0^t \int_\Omega a(x,\tau) \sum_{i,j=1}^{n} a_{ij}(x,\tau)\, u_{x_i\tau\tau} u_{x_j\tau\tau}\, dx\, d\tau -$$

$$- \int_0^t \int_\Omega \sum_{i,j=1}^{n} a_{ij}(x,\tau)\, a_{x_i}(x,\tau)\, u_{\tau\tau} u_{x_j\tau\tau}\, dx\, d\tau \leqslant$$

$$\leqslant c \int_0^t \int_\Omega \Big(|a(x,\tau)\, u_{\tau\tau}| + |a(x,\tau)\, \nabla u_{\tau\tau}| + |u_{\tau\tau}\, \nabla a(x,\tau)| \Big) \times$$

$$\times \int_\Omega \Big(R_3(y,\tau)\, |u(y,\tau)| + 2\, R_2(y,\tau)\, |u_\tau(y,\tau)| +$$

$$+ R_1(y,\tau)\, |u_{\tau\tau}(y,\tau)| \Big)\, dy\, ds\, d\tau + \int_0^t \int_\Omega B\, u\, A_0\, u_{\tau\tau}\, dx\, d\tau +$$

$$+ \int_0^t \int_\Omega f\, A_0\, u_{\tau\tau}\, dx\, d\tau.$$

Интегрируя по частям и оценивая выражение справа сверху, вводя обозначение $q(t) = \int_0^t \int_\Omega (A_0\, u_{\tau\tau})^2\, dx\, d\tau$ и замечая, что $q(0) = 0$, используя неравенства (2.1), (2.2), а также условия (1.5), (1.6), (2.5)–(2.8), получаем следующую оценку:

$$q(t) \leqslant \delta_4^2 \int_0^t \int_\Omega (A_0\, u_{\tau\tau})^2\, dx\, d\tau +$$

$$+ P_5 \Big(\sum_{i,j=1}^{n} \int_0^t \int_\Omega u^2_{x_i x_j}(x,\tau)\, dx\, d\tau + \int_0^t \int_\Omega |\nabla u_\tau(x,\tau)|^2\, dx\, d\tau +$$

$$+ \sum_{i,j=1}^{n} \int_0^t \int_\Omega u^2_{x_i\tau\tau}(x,\tau)\, dx\, d\tau + \int_0^t \int_\Omega u^2_{\tau\tau}\, dx\, d\tau + \int_0^t \int_\Omega u^2_\tau(x,\tau)\, dx\, d\tau +$$

$$+ \int_0^t \int_\Omega u^2(x,\tau)\, dx\, d\tau + \int_0^t \int_\Omega f^2(x,\tau)\, dx\, d\tau \Big) + \int_0^t \int_\Omega f\, A_0\, u_{\tau\tau}\, dx\, d\tau, \tag{4.9}$$

где число δ_4 — произвольное положительное число, P_5 есть число, определяющееся коэффициентами оператора B, а также областью Q_T и числом δ_4.

Тогда из (4.1)–(4.9) вытекает неравенство

$$\sum_{i=1}^{n} \int_\Omega u^2_{x_i t}(x,t)\, dx + \int_\Omega u_t^2(x,t)\, dx + \int_\Omega (A_0 u_t(x,t))^2 dx + \sum_{i=1}^{n} \int_0^t \int_\Omega u^2_{x_i\tau\tau}(x,\tau)\, dx\, d\tau +$$

$$+ \int_0^t \int_\Omega u^2_{\tau\tau}(x,\tau)\, dx\, d\tau + \int_0^t \int_\Omega (A_0 u_{\tau\tau}(x,\tau))^2\, dx\, d\tau \leqslant K_1\, \|f\|_{L_2(Q_T)}.$$

Эта оценка после перехода в ней к супремуму по $t \in [0,T]$ и дает требуемую оценку

$$\|u\|_V \leqslant K\, \|f\|_{L_2(Q_T)}. \tag{4.10}$$

Единственность решений краевой задачи (1.2)–(1.4) в пространстве V очевидна из априорной оценки (4.10). Теорема полностью доказана.

Заключение

В статье представлен новый результат по нелокальным задачам. Уравнения высокого порядка, нелокальные задачи для таких уравнений стали исследовать недавно. Получены условия на интегральное ядро в нелокальном условии. Вид условий отличается от таких в случае уравнений второго порядка, это вызвано большей сложностью получения априорных оценок. Результат обладает новизной и является важным шагом в исследовании уравнений высокого порядка.

Литература

[1] Кожанов А.И., Пулькина Л.С. Краевые задачи с интегральным граничным условием для многомерных гиперболических уравнений // Доклады РАН. 2005. Т. 404, № 5. С. 589–592. URL: https://www.elibrary.ru/item.asp?id=9157033.

[2] Кожанов А.И., Пулькина Л.С. О разрешимости краевой задачи с нелокальным граничным условием интегрального вида для многомерных гиперболических уравнений // Дифференц. уравнения. 2006. Т. 42, № 9. С. 1166–1179. URL: https://www.elibrary.ru/item.asp?id=9296592.

[3] Кожанов А.И., Пулькина Л.С. О разрешимости краевых задач с нелокальным граничным условием интегрального вида для многомерных гиперболических уравнений // Доклады Академии наук. 2005. Т. 404, № 5.

[4] Абдрахманов А.М., Кожанов А.И. Задача с нелокальным граничным условием для одного класса уравнений нечетного порядка // Изв. вузов. Математика. 2007. № 5. С. 3–12. URL: http://mi.mathnet.ru/ivm1386.

[5] Абдрахманов А.М. О разрешимости краевой задачи с интегро-дифференциальным граничным условием для некоторых классов уравнений составного типа // Мат. заметки ЯГУ. 2011. Т. 18, Вып. 2. С. 3–10. Available at: https://www.elibrary.ru/item.asp?id=18379047.

[6] Стретт Дж.В. (лорд Рэлей) Теория звука // ГИТТЛ. 1955. Т. 1. С. 273–274.

[7] Свешников А.Г., Боголюбов А.Н., Кравцов В.В. Лекции по математической физике. Москва: Изд-во МГУ, 1993. 313 с.

[8] Габов С.А., Свешников А.Г. Линейные задачи теории нестационарных внутренних волн. Москва: Наука. 1990. 344 с.

[9] Егоров И.Е., Федоров В.Е. Неклассические уравнения математической физики высокого порядка. Новосибирск: Изд-во ВЦ СО РАН, 1995. 133 с.

[10] Корпусов М.О. Разрушение в неклассических волновых уравнениях. Москва: URSS, 2010. 237 с.

[11] Дмитриев В.Б. Краевая задача с нелокальным граничным условием для уравнения четвертого порядка // Вестник СамГУ. Естественнонаучная серия. 2016. Вып. 3–4. С. 32–50. URL: https://journals.ssau.ru/est/article/view/4256.

[12] Попов Н.С. О разрешимости краевых задач для многомерных параболических уравнений четвертого порядка с нелокальным граничным условием интегрального вида // Математические заметки СВФУ. 2016. Т. 23, № 1. С. 79–86. URL: http://mi.mathnet.ru/svfu17.

[13] Попов Н.С. О разрешимости краевой задачи для многомерных псевдогиперболических уравнений с нелокальным граничным условием интегрального вида // Математические заметки СВФУ. 2014. Т. 21, № 2. С. 69–80. URL: https://www.s-vfu.ru/universitet/rukovodstvo-i-struktura/instituty/niim/mzsvfu/issues/2014-2/69-80.pdf.

[14] Попов Н.С. Разрешимость краевой задачи для псевдопараболического уравнения с нелокальными интегральными условиями // Дифференциальные уравнения. 2015. Т. 51, № 3. С. 359–372. DOI: https://doi.org/10.1134/S0374064115030073.

[15] Кожанов А.И., Дюжева А.В. Нелокальные задачи с интегральным смещением для параболических уравнений высокого порядка // Известия Иркутского государственного университета. Естественнонаучная серия. Серия Математика. 2021. Т. 36. С. 14–28. DOI: https://doi.org/10.26516/1997-7670.2021.36.14.

[16] Юлдашев Т.К. Нелокальная краевая задача для неоднородного псевдопараболического интегро-дифференциального уравнения с вырожденным ядром // Вестн. Волгогр. гос. ун-та. Сер. 1. Мат. Физ. 2017. Вып. 1 (38). С. 42–54. DOI: https://doi.org/10.15688/jvolsu1.2017.1.5.

[17] Юлдашев Т.К. Об одной краевой задаче для трехмерного аналога дифференциального уравнения Буссинеска // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. 2016. Т. 158, Кн. 3. С. 424–433. URL: http://mi.mathnet.ru/uzku1377.

[18] Юлдашев Т.К. Об одном интегро-дифференциальном уравнении Фредгольма в частных производных третьего порядка // Изв. вузов. Матем. 2015. № 9. С. 74–79. URL: http://mi.mathnet.ru/ivm9038.

[19] Бейлин А.Б. Пулькина Л.С. Задачи о колебаниях стержня с нелинейным затуханием второго порядка // Вестник Самарского университета. Естественнонаучная серия. 2015. № 3 (125). С. 9–20.

[20] Ладыженская О.А. Краевые задачи математической физики. Москва: Наука, 1973. 408 с.

[21] Ладыженская О.А., Уральцева Н.Н. Линейные и квазилинейные уравнения эллиптического типа. Москва: Наука, 1973.

[22] Гординг Л. Задача Коши для гиперболических уравнений. Москва: Изд. ИЛ, 1961. 122 с.

[23] Треногин В.А. Функциональный анализ. Москва: Наука, 1980.

[24] Якубов С.Я. Линейные дифференциально-операторные уравнения и их приложения. Баку: Элм, 1985.

Scientific article

DOI: 10.18287/2541-7525-2021-27-1-15-28

Submited: 12.01.2021
Revised: 17.02.2021
Accepted: 28.02.2021

V.B. Dmitriev
E-mail: dmitriev_v.b@mail.ru. ORCID: https://orcid.org/0000-0002-9788-7036

BOUNDARY VALUE PROBLEM WITH A NONLOCAL BOUNDARY CONDITION OF INTEGRAL FORM FOR A MULTIDIMENSIONAL EQUATION OF IV ORDER

ABSTRACT

The aim of this paper is to study the solvability of solution of non-local problem with integral condition in spatial variables for high-order linear equation in the classe of regular solutions (which have all the squared derivatives generalized by S.L. Sobolev that are included in the corresponding equation). It is indicated that at first similar problems were studied for high-order equations either in the one-dimensional case, or under certain conditions of smallness by the value of T. A list of new works for the multidimensional case is also given. In this paper, we present new results on the solvability of non-local problem with integral spatial variables for high-order equation a) in the multidimensional case with respect to spatial variables; b) in the absence of smallness conditions by the value T; however, this condition exists for the kernel $K(x, y, t)$. The research method is based on obtaining a priori estimates of the solution of the problem, which implies its existence and uniqueness in a given space.

Key words: boundary value problem; non-local condition; high-order equation; priori estimates; integral boundary conditions; Boussinesq equation; regular solutions; uniqueness; existence.

Citation. Dmitriev V.B. Boundary value problem with a nonlocal boundary condition of integral form for a multidimensional equation of IV order. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2021, vol. 27, no. 1, pp. 15–28. DOI: http://doi.org/10.18287/2541-7525-2021-27-1-15-28. (In Russ.)

Information about the conflict of interests: author and reviewers declare no conflict of interests.

© Dmitriev V.B., 2021

Victor Borisovich Dmitriev — Candidate of Physical and Mathematical Sciences.

References

[1] Kozhanov A.I., Pul'kina L.S. Boundary value problems with integral conditions for multidimensional hyperbolic equations. *Doklady Mathematics*, 2005, vol. 72, no. 2, pp. 743–746. Available at: https://www.elibrary.ru/item.asp?id=13480468 [English; Russian original]

[2] Kozhanov A.I., Pul'kina L.S. On the solvability of boundary value problems with a nonlocal boundary condition of integral form for multidimensional hyperbolic equations. *Differential Equations*, 2006, vol. 42, no. 9, pp. 1233–1246. DOI: http://doi.org/10.1134/S0012266106090023. [Englsh; Russian original]

[3] *Kozhanov A.I., Pul'kina L.S.* On the solvability of boundary value problems with a nonlocal boundary condition of integral form for multidimensional hyperbolic equations. *Doklady Mathematics*, 2005, vol. 404, no. 5. (In Russ.)

[4] Abdrakhmanov A.M., Kozhanov A.I. A problem with a non-local boundary condition for one class of odd-order equations. *Russian Mathematics*, 2007, vol. 51, no. 5, pp. 1–10. DOI: https://doi.org/10.3103/S1066369X07050015. (In Russ.)

[5] Abdrakhmanov A.M. On the solvability of boundary value problem with integrodifferential boundary condition for some classes of composite type equations. *Mathematical Notes of YSU*, 2011, vol. 18, Issue 2, pp. 3–10. Available at: https://www.elibrary.ru/item.asp?id=18379047. (In Russ.)

[6] Rayleigh J.W.S. Theory of sound. Moscow: GITTL, 1955, vol. 1, pp. 273—274. (In Russ.)

[7] Sveshnikov A.G., Bogolyubov A.N., Kravtsov V.V. Lectures on mathematical physics: textbook. Moscow: Izd-vo MGU, 1993, 313 p. (In Russ.)

[8] Gabov S.A., Sveshnikov A.G. Linear problems in the theory of nonstationary internal waves. Moscow: Nauka, 1990, 344 p. (In Russ.)

[9] Egorov I.E., Fedorov V.E. High-order non-classical equations of mathematical physics. Novosibirsk: Izd-vo VTs SO RAN, 1995, 133 p. (In Russ.)

[10] Korpusov P.O. Destruction in nonclassical wave equations. Moscow: URSS, 2010, 237 p. (In Russ.)

[11] Dmitriev V.B. A nonlocal problem with integral condition for a fourth order equation. *Vestnik Samarskogo Gosuniversiteta. Estestvennonauchnaia seriia = Vestnik of Samara State University. Natural Science Series*, 2016, no. 3-4, pp. 32–50. Available at: https://journals.ssau.ru/est/article/view/4256. (In Russ.)

[12] Popov N.S. On the solvability of boundary value problems for multidimensional parabolic equations of fourth order with nonlocal boundary condition of integral form. *Mathematical Notes of NEFU*, 2016, vol. 23, no. 1, pp. 79–86. Available at: http://mi.mathnet.ru/svfu17. (In Russ.)

[13] Popov N.S. On the solvability of boundary value problems for higher-dimensional pseudohyperbolic equations with a nonlocal boundary condition in integral form. *Mathematical Notes of NEFU*, 2014, vol. 21, no. 2, pp. 69–80. Available at: https://www.s-vfu.ru/universitet/rukovodstvo-i-struktura/instituty/niim/mzsvfu/issues/2014-2/69-80.pdf. (In Russ.)

[14] Popov N.S. Solvability of a boundary value problem for a pseudoparabolic equation with nonlocal integral conditions. *Diferential Equations*, 2015, vol. 51, no. 3, pp. 362–375. DOI: http://doi.org/10.1134/S0012266115030076 [English; Russian original]

[15] Kozhanov A.I., Dyuzheva A.V. Non-local problems with integral displacement for high-order parabolic equations. *The Bulletin of Irkutsk State University. Series Mathematics*, 2021, vol. 36, pp. 14–28. DOI: https://doi.org/10.26516/1997-7670.2021.36.14. (In Russ.)

[16] Yuldashev T.K. Nonlocal boundary value problem for a nonhomogeneous pseudoparabolic-type integro-differential equation with degenerate kernel. *Vestnik Volgogradskogo gosudarstvennogo universiteta. Seriya 1. Mathematica. Physica = Science Journal of Volgograd State University. Mathematics. Physics*, 2017, issue 1 (38), pp. 42–54. DOI: https://doi.org/10.15688/jvolsu1.2017.1.5. (In Russ.)

[17] Yuldashev T.K. On the boundary value problem for a three dimensional analog of the Boussinesq differential equation. *Uchenye Zapiski Kazanskogo Universiteta. Seriya Fiziko-Matematicheskie Nauki*, 2016, vol. 158, book 3, pp. 424-–433. Available at: http://mi.mathnet.ru/uzku1377. (In Russ.)

[18] Yuldashev T.K. A certain Fredholm partial integro-differential equation of the third order. *Russian Mathematics*, 2015, vol. 59, no. 9, pp. 62—66. DOI: https://doi.org/10.3103/S1066369X15090091. [English; Russian original]

[19] Beylin A.B., Pulkina L.S. Problem on vibration of a bar with nonlinear second-order boundary damping. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2015, no. 3 (125), pp. 9-–20. Available at: https://journals.ssau.ru/est/article/view/4487. (In Russ.)

[20] *Ladyzhenskaya O.A.* Boundary value problems of mathematical physics. Moscow: Nauka, 1973, 408 p. (In Russ.)

[21] Ladyzhenskaya O.A., Uraltseva N.N. Linear and quasi-linear equations of elliptic type. Moscow: Nauka, 1973, 538 p. (In Russ.)

[22] *Gording L.* The Cauchy problem for hyperbolic equations. Leningrad: Moscow, 1961, 122 p. (In Russ.)

[23] Trenogin V.A. Functional analysis. Moscow: Nauka, 1980, 488 p. (In Russ.)

[24] Yakubov S.Ya. Linear differential-operator equations and their applications. Baku: Elm, 1985. (In Russ.)

Scientific article
DOI: 10.18287/2541-7525-2021-27-1-29–43

Submited: 15.01.2021
Revised: 17.02.2021
Accepted: 28.02.2021

E. Providas
University of Thessaly, Larissa, Greece
E-mail: providas@uth.gr. ORCID: https://orcid.org/0000-0002-0675-4351
L.S. Pulkina
Samara National Research University, Samara, Russian Federation
E-mail: louise@samdiff.ru. ORCID: https://orcid.org/0000-0001-7947-612
I.N. Parasidis
University of Thessaly, Larissa, Greece
E-mail: paras@teilar.gr. ORCID: https://orcid.org/0000-0002-7900-9256

FACTORIZATION OF ORDINARY AND HYPERBOLIC INTEGRO-DIFFERENTIAL EQUATIONS WITH INTEGRAL BOUNDARY CONDITIONS IN A BANACH SPACE

ABSTRACT

The solvability condition and the unique exact solution by the universal factorization (decomposition) method for a class of the abstract operator equations of the type

$$B_1 u = \mathcal{A}u - S\Phi(A_0 u) - GF(\mathcal{A}u) = f, \quad u \in D(B_1),$$

where $\mathcal{A}, A_0$ are linear abstract operators, G, S are linear vectors and Φ, F are linear functional vectors is investigagted. This class is useful for solving Boundary Value Problems (BVPs) with Integro-Differential Equations (IDEs), where $\mathcal{A}, A_0$ are differential operators and $F(\mathcal{A}u), \Phi(A_0 u)$ are Fredholm integrals. It was shown that the operators of the type B_1 can be factorized in the some cases in the product of two more simple operators B_G, B_{G_0} of special form, which are derived analytically. Further the solvability condition and the unique exact solution for $B_1 u = f$ easily follow from the solvability condition and the unique exact solutions for the equations $B_G v = f$ and $B_{G_0} u = v$.

Key words: correct operator; factorization (decomposition) method; Fredholm integro-differential equations; initial problem; nonlocal boundary value problem with integral boundary conditions.

Citation. Providas E., Pulkina L.S., Parasidis I.N. Factorization of ordinary and hyperbolic integro-differential equations with integral boundary conditions in a Banach space. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2021, vol. 27, no. 1, pp. 29–43. DOI: http://doi.org/10.18287/2541-7525-2021-27-1-29–43.

Information about the conflict of interests: authors and reviewers declare no conflict of interests.

© Providas E., 2021
Efthimios Providas — Candidate of Technical Sciences, associate professor, University of Thessaly, Larissa, 41110, Greece.
© Pulkina L.S., 2021
Ludmila Stepanovna Pulkina — Doctor of Physical and Mathematical Sciences, professor, Department of Differential Equations and Control Theory, Samara National Research University, 34, Moskovskoye shosse, 443086, Russian Federation.
© Parasidis I.N., 2021
Ioannis Nestorios Parasidis — Candidate of Technical Sciences, associate professor, University of Thessaly, Larissa, 41110, Greece.

1. Initial Position

Integro-differential equations play an important role in characterizing many physical, biological, social and engineering problems and are often solved by factorization (decomposition) methods. The factorization methods have applications in biology, ecology, population dynamics, mathematics of financial derivatives, quantum physics, hydrodynamics, gas dynamics, in transport theory, electromagnetic theory, mechanics and chemistry [1–10]. Factorization Methods successfully are used in pure mathematics for solving linear and nonlinear ordinary and partial differential and Volterra-Fredholm integro-differential equations, integro-differential equations of fractional order, fuzzy Volterra-Fredholm integral equations and delay differential equations [11–20]. There are well-known decomposition (factorization) methods: Domain decomposition method, the natural transform decomposition method, the Adomian decomposition method, Modified Adomian decomposition method and the Combined Laplace transform-Adomian decomposition method, which use the so-called Adomyan polynomials or iterations to obtain an n-term approximation of solution, whereas the proposed in this paper factorization method gives the unique exact solution in the closed form. Furthermore it is universal because can be applied in the investigation of Fredholm integro-differential equations, both ordinary and partial.

There are many papers are devoted to investigation of the uniqueness of the solution to nonlocal boundary value problems with integral boundary conditions for hyperbolic differential equation [21–25]. Finding of the exact solution in the general case is the difficult task. We by the universal factorization method find the solvability condition and a unique solution to a nonlocal BVP with integral boundary conditions for Fredholm ordinary integro-differential and integro-hyperbolic differential equations of the type $B_1u = f$. It is the aim of this paper to reappraise the factorization method for integro-differential equations of type $B_1u = f$. This paper is a generalization of the article [26], where by factorization method were stydied the solvability condition and a unique solution to the correct self-adjoint abstract equation of the type $B_1u = f$ in terms of a Hermitian matrix in a Hilbert space.

The quadratic factorization methods was applied to some BVPs with integro-differential equations in the case of a Banach space in [27–29].

It is well known that the class of the operators which can be factorized as a superposition of two more simple operators is not wide. But if the operator can be factorized, then the solvability condition and the solution of the given problem are essentially simpler than in the general case without factorization. The paper is organized as follows. In Section 2 we develop the theory for the solution of the problem $B_1x = f$ when $B_1 = BB_0$. Further by factorization method we solve a nonlocal boundary value problem with integral boundary conditions for Fredholm integro-hyperbolic differential equation. Finally, we give two examples of integro-differential equations demonstrating the power and usefulness of the methods presented.

Throughout this paper we use the following terminology and notation. By X, Y we denote the complex Banach spaces and by X^* the adjoint space of X, i.e. the set of all complex-valued linear and bounded functionals on X. We denote by $f(u)$ the value of f on $u \in X$. We write $D(A)$ and $R(A)$ for the domain and the range of the operator $A : X \to Y$, respectively. An operator A_2 is said to be an *extension* of an operator A_1, or A_1 is said to be a *restriction* of A_2, in symbol $A_1 \subset A_2$, if $D(A_2) \supseteq D(A_1)$ and $A_1x = A_2x$, for all $x \in D(A_1)$. An operator $A : X \to Y$ is said to be *injective or uniquelly solvable* if for all $u_1, u_2 \in D(A)$ such that $Au_1 = Au_2$, follows that $u_1 = u_2$. Remind that a linear operator A is injective if and only if $\ker A = \{0\}$. An operator $A : X \to Y$ is called *surjective* or *everywhere solvable* if $R(A) = Y$. The operator $A : X \to Y$ is called *bijective* if A is both injective and surjective. Lastly, A is said to be *correct* if A is bijective and its inverse A^{-1} is bounded on Y. If $g_i \in X$ and $\Psi_i \in X^*, i = 1, \dots, m$, then we denote by $g = (g_1, \dots, g_m)$, $\Psi = \mathrm{col}(\Psi_1, \dots, \Psi_m)$ and $\Psi(u) = \mathrm{col}(\Psi_1(u), \dots, \Psi_m(u))$ and write $g \in X_m$, $\Psi \in X_m^*$. We will denote by $\Psi(g)$ the $m \times m$ matrix whose i, j-th entry $\Psi_i(g_j)$ is the value of functional Ψ_i on element g_j. Note that $\Psi(gC) = \Psi(g)C$, where C is a $m \times k$ constant matrix. We will also denote by 0_m the zero and by I_m the identity $m \times m$ matrices. By $\mathbf{0}$ we will denote the zero column vector.

2. Factorization of integro-differential equations in a Banach space

We remind first the following Theorem 1 from [29].

Theorem 2.1. *Let A be a bijective operator on a Banach space X, the components of the vectors $G = (g_1, ..., g_m)$, $F = col(F_1, ...F_m)$ arbitrary elements of X and X^*, respectively and the operator $B_G : X \to X$ be defined by*

$$B_Gu = Au - GF(Au) = f, \quad D(B_G) = D(A), \quad f \in X. \tag{2.1}$$

Then the following statements are true:

(i) The operator B_G is bijective on X if and only if

$$\det L = \det[I_m - F(G)] \neq 0, \tag{2.2}$$

and the unique solution to boundary value problem (2.1), for any $f \in X$, is given by the formula

$$u = B_G^{-1} f = A^{-1} f + A^{-1} G[I_m - F(G)]^{-1} F(f). \tag{2.3}$$

(ii) If in addition the operator A is correct, then B_G is correct.

Now, by using the above theorem we prove the following theorem which is useful for solving integro-differential equations by factorization method.

Theorem 2.2. *Let X be a Banach space, the vectors $G_0 = (g_1^{(0)}, ..., g_m^{(0)})$, $G = (g_1, ..., g_m)$, $S = (s_1, ..., s_m) \in X^m$, the components of the vectors $F = col(F_1, ..., F_m)$ and $\Phi = col(\phi_1, ..., \phi_m)$ belong to X^* and the operators $B_{G_0}, B_G, B_1 : X \to X$ defined by*

$$B_{G_0} u = A_0 u - G_0 \Phi(A_0 u) = f, \qquad D(B_{G_0}) = D(A_0), \tag{2.4}$$

$$B_G u = Au - GF(Au) = f, \qquad D(B_G) = D(A), \tag{2.5}$$

$$B_1 u = AA_0 u - S\Phi(A_0 u) - GF(AA_0 u) = f, \quad D(B_1) = D(AA_0) \tag{2.6}$$

where A_0 and A are linear correct operators on X and $G_0 \in D(A)^m$. Then the following statements are satisfied:
(i) If

$$S \in R(B_G)^m \quad \text{and} \quad S = B_G G_0 = AG_0 - GF(AG_0), \tag{2.7}$$

then the operator B_1 can be factorised in $B_1 = B_G B_{G_0}$.
(ii) If in addition the components of the vector $\Phi = (\Phi_1, ..., \Phi_m)$ are linearly independent elements of X^* and the operator B_1 can be factorised in $B_1 = B_G B_{G_0}$, then (2.7) is fulfilled.
(iii) If the operator B_1 can be factorised in $B_1 = B_G B_{G_0}$, then B_1 is correct if and only if the operators B_{G_0} and B_G are correct which means that

$$\det L_0 = \det[I_m - \Phi(G_0)] \neq 0 \quad \text{and} \quad \det L = \det[I_m - F(G)] \neq 0. \tag{2.8}$$

(iv) If the operator B_1 has the factorization in $B_1 = B_G B_{G_0}$ and is correct, then the unique solution of (2.6) is

$$\begin{aligned} u = B_1^{-1} f = \quad & A_0^{-1} A^{-1} f + \left[A_0^{-1} A^{-1} G + A_0^{-1} G_0 L_0^{-1} \Phi(A^{-1} G)\right] \times \\ & \times L^{-1} F(f) + A_0^{-1} G_0 L_0^{-1} \Phi(A^{-1} f). \end{aligned} \tag{2.9}$$

Proof. (i) Taking into account that $G_0 \in D(A)^m$ and (2.4)–(2.6) we get

$$\begin{aligned} D(B_G B_{G_0}) \quad &= \{u \in D(B_{G_0}) : \, B_{G_0} u \in D(B_G)\} = \\ &= \{u \in D(A_0) : \, A_0 u - G_0 \Phi(A_0 u) \in D(A)\} = \\ &= \{u \in D(A_0) : \, A_0 u \in D(A)\} = D(AA_0) = D(B_1). \end{aligned}$$

So $D(B_1) = D(B_G B_{G_0})$. Let $y = B_{G_0} u$. Then for each $u \in D(AA_0)$ since (2.5) and (2.4) we have

$$\begin{aligned} B_G B_{G_0} u \quad &= B_G y = Ay - GF(Ay) = \\ &= A[A_0 u - G_0 \Phi(A_0 u)] - GF\left(A[A_0 u - G_0 \Phi(A_0 u)]\right) = \\ &= AA_0 u - AG_0 \Phi(A_0 u) - GF(AA_0 u) + GF(AG_0)\Phi(A_0 u) = \\ &= AA_0 u - [AG_0 - GF(AG_0)]\Phi(A_0 u) - GF(AA_0 u) = \\ &= AA_0 u - B_G G_0 \Phi(A_0 u) - GF(AA_0 u), \end{aligned} \tag{2.10}$$

where the relation $B_G G_0 = AG_0 - GF(AG_0)$ follows from (2.5) if instead of u we take G_0. By comparing (2.10) with (2.6), it is easy to verify that $B_1 u = B_G B_{G_0} u$ for each $u \in D(AA_0)$ if a vector S satisfies (2.7).
(ii) Let the operator B_1 can be factorized in $B_1 = B_G B_{G_0}$. Then by comparing (2.10) with (2.6) we obtain

$$(B_G G_0 - S)\Phi(A_0 u) = 0. \tag{2.11}$$

Because of the correctness of operators A, A_0 and the linear independence of $\Phi_1, ..., \Phi_m$, there exists a system $u_1, ..., u_m \in D(AA_0)$ such that $\Phi(A_0 u_0) = I_m$ where $u_0 = (u_1, ..., u_m)$. By substituting $u = u_0$ into (2.11) we get $S = B_G G_0$. Hence $S \in R(B_G)^m$ and $S = B_G G_0 = AG_0 - GF(AG_0)$.
(iii) Let the operator B_1 be defined by (2.6) where $S = B_G G_0$. Then Equation (2.6) can be equivalently represented in matrix form:

$$B_1 u = AA_0 u - (B_G G_0, G) \begin{pmatrix} \Phi(A^{-1} AA_0 u) \\ F(AA_0 u) \end{pmatrix} = f \tag{2.12}$$

or

$$B_1 u = \mathcal{A}u - \mathcal{G}\mathcal{F}(\mathcal{A}u) = f, \quad D(B_1) = D(\mathcal{A}), \tag{2.13}$$

where $\mathcal{A} = AA_0$, $\mathcal{G} = (B_G G_0, G)$, $\mathcal{F} = \mathrm{col}(\hat{\Phi}, F)$, $\mathcal{F}(v) = \begin{pmatrix} \hat{\Phi}(v) \\ F(v) \end{pmatrix} = \begin{pmatrix} \Phi(A^{-1}v) \\ F(v) \end{pmatrix}$. Notice that the operator $\mathcal{A} = AA_0$ is correct, because of A and A_0 are the correct operators and that the functional vector $\mathcal{F}$ is bounded, since the vector $\hat{\Phi}$ is bounded as a superposition of a bounded functional Φ and a bounded operator A^{-1}. Then we apply Theorem 2.1. By this theorem the operator B_1 is correct if and only if

$$\begin{aligned}
\det L_1 = \ & \det[I_{2m} - \mathcal{F}(\mathcal{G})] = \det\left[\begin{pmatrix} I_m & 0_m \\ 0_m & I_m \end{pmatrix} - \begin{pmatrix} \hat{\Phi}(B_G G_0) & \hat{\Phi}(G) \\ F(B_G G_0) & F(G) \end{pmatrix}\right] = \\
& = \det \begin{pmatrix} I_m - \hat{\Phi}(AG_0 - GF(AG_0)) & -\hat{\Phi}(G) \\ -[F(AG_0 - GF(AG_0))] & I_m - F(G) \end{pmatrix} = \\
& = \det \begin{pmatrix} I_m - \Phi(G_0 - A^{-1}GF(AG_0)) & -\Phi(A^{-1}G) \\ -[F(AG_0 - GF(AG_0))] & I_m - F(G) \end{pmatrix} = \\
& = \det \begin{pmatrix} I_m - \Phi(G_0) + \Phi(A^{-1}G)F(AG_0) & -\Phi(A^{-1}G) \\ -F(AG_0) + F(G)F(AG_0) & I_m - F(G) \end{pmatrix} \neq 0.
\end{aligned}$$

Multiplying from the left the elements of the second column by $F(AG_0)$ and adding to the corresponding elements of the first column of the determinant L_1, by Remark 1, [31] we get

$$\begin{aligned}
\det L_1 = \ & \det \begin{pmatrix} I_m - \Phi(G_0) & -\Phi(A^{-1}G) \\ 0_m & I_m - F(G) \end{pmatrix} = \det[I_m - \Phi(G_0)] \det[I_m - F(G)] \\
& = \det L_0 \det L \neq 0.
\end{aligned}$$

So we proved that the operator B_1 is correct if and only if (2.8) is fulfilled.
(iv) Let $u \in D(AA_0)$ and $B_G B_{G_0} u = f$. By Theorem 2.1 (ii) since B_G, B_{G_0} are correct operators, we obtain

$$\begin{aligned}
& B_{G_0} u = B_G^{-1} f = A^{-1} f + A^{-1} G L^{-1} F(f), \\
& u = B_{G_0}^{-1}\left(A^{-1} f + A^{-1} G L^{-1} F(f)\right).
\end{aligned}$$

In the last equation we denote by $g = A^{-1} f + A^{-1} G L^{-1} F(f)$. Bu using again Theorem 2.1 (ii), with A_0, G_0, Φ, L_0, in place of A, G, F, L respectively, we get

$$\begin{aligned}
& u = B_{G_0}^{-1} g = A_0^{-1} g + A_0^{-1} G_0 L_0^{-1} \Phi(g) = A_0^{-1}\big(A^{-1} f + A^{-1} G L^{-1} F(f)\big) + \\
& + A_0^{-1} G_0 L_0^{-1} \Phi\left(A^{-1} f + A^{-1} G L^{-1} F(f)\right) = A_0^{-1} A^{-1} f + A_0^{-1} A^{-1} G L^{-1} F(f) + \\
& + A_0^{-1} G_0 L_0^{-1}\big[\Phi(A^{-1} f) + \Phi(A^{-1} G) L^{-1} F(f)\big]
\end{aligned}$$

which implies (2.9). The theorem is proved. □

The next theorem is useful for applications.

Theorem 2.3. *Let the space X and the vectors F, Φ be defined as in Theorem 2.2, the vectors $G = (g_1, ..., g_m)$, $S = (s_1, ..., s_m) \in X^m$ and the operator $B_1 : X \to X$ by*

$$B_1 u = \mathcal{A}u - S\Phi(A_0 u) - GF(\mathcal{A}u) = f, \quad x \in D(B_1) \tag{2.14}$$

where $A_0 : X \to X$ is a correct m-order differential operator and $\mathcal{A}$ is a n-order differential operator, $m < n$. Then the next statements are fulfilled:
(i) if there exist a $n - m$ order differential operator $A : X \to X$, such that

$$\mathcal{A} = AA_0, \quad D(B_1) = D(AA_0), \tag{2.15}$$

and a vector $G_0 \in D(A)$, satisfying

$$AG_0 - GF(AG_0) = S, \tag{2.16}$$

then the operator B_1 can be factorized into $B_1 = B_G B_{G_0}$, where B_{G_0} and B_G are given by (2.4) and (2.5) respectively, B_G is determined by A and G, F from (2.14), (2.15) and lastly, the operator B_{G_0} by A_0, Φ and G_0 from (2.14) and (2.16),
(ii) if there exists a bijective $n - m$ order differential operator $A : X \to X$, satisfying (2.15) and

$$\det L = \det[I_m - F(G)] \neq 0, \tag{2.17}$$

then the operator B_1 is factorized in $B_1 = B_G B_{G_0}$, where the operators B_{G_0}, B_G, A_0, A, the vectors G, F, Φ are determined as in (i) and

$$G_0 = A^{-1} S + A^{-1} G L^{-1} F(S). \tag{2.18}$$

(iii) if in addition to (ii) A is correct, then B_1 is correct if and only if

$$\det L_0 = \det[I_m - \Phi(G_0)] = \det[I_m - \Phi(\widehat{A}^{-1}S) - \Phi(\widehat{A}^{-1}G)L^{-1}F(S)] \neq 0, \tag{2.19}$$

and the problem (2.14)-(2.16) has the unique solution given by (2.9).

Proof (i) If there there exist a $n-m$ order differential operator A and a vector G_0 satisfying (2.15) and (2.16), then from (2.14) we get

$$B_1 u = AA_0 u - S\Phi(A_0 u) - GF(AA_0 u) = f, \quad u \in D(AA_0). \tag{2.20}$$

From (2.20) we take a triple of elements, the operator A and vectors G, F, and construct the operator B_G according to the formula (2.5). To determine the operator B_{G_0} by formula (2.4), we take from (2.20) the operator A_0 and the vector Φ, whereas as G_0 we take any solution G_0 of Equation (2.16). We proved in the previous theorem (i) that $D(B_G B_{G_0}) = D(AA_0) = D(B_1)$. Substituting (2.16) into (2.20), for every $u \in D(B_1)$ we get

$$\begin{aligned} B_1 u &= AA_0 u - [AG_0 - GF(AG_0)]\,\Phi(A_0 u) - GF(AA_0 u) = B_G A_0 u - B_G G_0 \Phi(A_0 u) = \\ &= B_G\,[A_0 u - G_0 \Phi(A_0 u)] = B_G B_{G_0} u. \end{aligned}$$

Thus $B_1 = B_G B_{G_0}$.
(ii) As in the proof of (i) we construct the operators B_G, B_{G_0}. By Theorem 2.1, since (2.17), the operator B_G is correct and Equation (2.16) can be presented by $B_G G_0 = S$. Then $G_0 = B_G^{-1} S$. The last equation by Corollary 2.1, implies the unique vector G_0 by (2.18). Further as in the proof of (i) we get the factorization $B_1 = B_G B_{G_0}$, where B_{G_0} is unique.
(iii) If (2.17), (2.18) hold true, then by statements (i), (ii), B_1 can be factorized in $B_1 = B_G B_{G_0}$. By Theorem 2.2 (iii), B_1 is correct if and only if (2.8) holds or, taking into account (2.17) and (2.18), if and only if $\det L_0 = \det[I_m - \Phi(G_0)] \neq 0$, or if and only if (2.19) is fulfilled. The last inequality immediately follows by substitution (2.18) into $\det L_0 = \det[I_m - \Phi(G_0)]$. Since B_1 is correct and factorized in $B_1 = B_G B_{G_0}$, by Theorem 2.2 (iv), we obtain the unique solution (2.9) to the problem (2.14)-(2.16). So the theorem is proved. □

Example 2.4. Let $u(x) \in C^2[0,1]$. Then the problem

$$\begin{gathered} u''(t) - t\int_0^1 tu'(t)dt - t^2\int_0^1 t^3 u''(t)dt = 2t+1, \\ u(0) + u(1) = 0, \quad u'(0) - 2u'(1) = 0, \end{gathered} \tag{2.21}$$

is correct on $C[0,1]$ and its unique solution is given by the formula

$$u(t) = \frac{261377 - 665232t + 103608t^2 + 30080t^3 + 8790t^4}{207216}. \tag{2.22}$$

Proof. First we need to find the operators B_1, A, A_0 and check the condition $D(B_1) = D(AA_0)$. If we compare equation (2.21) with equation (2.14), (2.15), it is natural to take

$$B_1 u(t) = u''(t) - t\int_0^1 tu'(t)dt - t^2\int_0^1 t^3 u''(t)dt = 2t+1, \tag{2.23}$$

$$D(B_1) = \{u(t) \in C^2[0,1] : u(0) + u(1) = 0, \quad u'(0) - 2u'(1) = 0\},$$

$$\begin{gathered} \mathcal{A}u = AA_0 u = u''(t), \\ D(B_1) = \{u(t) \in C^2[0,1] : u(0) + u(1) = 0, \quad u'(0) - 2u'(1) = 0\}, \\ A_0 u(t) = u'(t), \quad D(A_0) = \{u(t) \in C^1[0,1] : u(0) = -u(1)\}, \end{gathered} \tag{2.24}$$

$$\Phi(A_0 u) = \int_0^1 tu'(t)dt, \quad F(AA_0 u) = \int_0^1 t^3 u''(t)dt, \tag{2.25}$$

$S = t$, $G = t^2$. Denote $A_0 u(t) = u'(t) = y(t) = y$. Then from (2.24) we have $y \in D(A)$, $AA_0 u = (u'(t))' = y'(t) = Ay(t)$, $y(0) - 2y(1) = 0$. So we proved that

$$Ay = y'(t), \quad D(A) = \{y(t) \in C^1[0,1] : y(0) - 2y(1) = 0\}.$$

Then by definition

$$\begin{aligned} D(AA_0) &= \{u(t) \in D(A_0) : A_0 u(t) \in D(A)\} = \\ &= \{u(t) \in C^1[0,1] : u(0) = -u(1),\, u'(t) \in C^1[0,1],\, u'(0) - 2u'(1) = 0\} = \\ &= \{u(t) \in C^2[0,1] : u(0) + u(1) = 0, \quad u'(0) - 2u'(1) = 0\} = D(B_1). \end{aligned}$$

So $D(B_1) = D(AA_0)$. It is easy to verify that the operators A, A_0 are correct on $C[0,1]$ and for every $f(t) \in C[0,1]$ the corresponding inverse operators are defined by

$$A^{-1}f(t) = \int_0^t f(s)ds - 2\int_0^1 f(s)ds, \tag{2.26}$$

$$A_0^{-1}f(t) = \int_0^t f(s)ds - \tfrac{1}{2}\int_0^1 f(s)ds. \tag{2.27}$$

From (2.25) we have

$$\Phi(f) = \int_0^1 sf(s)ds, \quad F(f) = \int_0^1 s^3 f(s)ds. \tag{2.28}$$

Then $F(G) = \int_0^1 s^3 s^2 ds = \frac{1}{6}$, $F(S) = \int_0^1 s^3 s ds = \frac{1}{5}$,
$\det L = \det[I_m - F(G)] = 1 - 1/6 = 5/6$, $L^{-1} = 6/5$,

$$A^{-1}S = \int_0^t sds - 2\int_0^1 sds = \frac{t^2}{2} - 1, \quad A^{-1}G = \int_0^t s^2 ds - 2\int_0^1 s^2 ds = \frac{t^3}{3} - \frac{2}{3},$$

$$G_0 = A^{-1}S + A^{-1}GL^{-1}F(S) = \frac{t^2}{2} - 1 + \left(\frac{t^3}{3} - \frac{2}{3}\right)\frac{6}{5}\frac{1}{5} = \frac{1}{50}(4t^3 + 25t^2 - 58).$$

Taking into account (2.28) we obtain

$$\Phi(G_0) = \frac{1}{50}\int_0^1 s(4s^3 + 25s^2 - 58)ds = -\frac{439}{1000}.$$

Since $\det L_0 = \det[I_m - \Phi(G_0)] = \frac{1439}{1000} \neq 0$ then, by Theorem 2.3 (iii), Problem (2.23) or (2.21) is correct. By (2.27) we calculate

$$A_0^{-1}G_0 = \frac{73}{150} - \frac{29t}{25} + \frac{t^3}{6} + \frac{t^4}{50}, \quad A_0^{-1}A^{-1}G = \frac{7}{24} - \frac{2t}{3} + \frac{t^4}{12}$$

and for $f(t) = 2t + 1$ by (2.26)-(2.28) we obtain

$$A^{-1}f = -4 + t + t^2, \quad A_0^{-1}A^{-1}f = \frac{19}{12} - 4t + \frac{t^2}{2} + \frac{t^3}{3}, \quad F(f) = \frac{13}{20}, \quad \Phi(A^{-1}f) = -\frac{17}{12}$$

Substituting these values into (2.9) we obtain the unique solution of (2.23), which is given by (2.22). □

Example 2.5. Let $u(x) \in C^3[0,1]$. Then the problem

$$u'''(x) - 8x^2\int_0^1 tu'(t)dt - (3x+1)\int_0^1 t^2u'''(t)dt = 2x^2 - 6x + 4, \tag{2.29}$$
$$u(0) = 2\int_0^1 u(t)dt, \quad u'(0) = -u'(1),\ u''(0) = -u''(1),$$

is uniquely solvable on $C[0,1]$ and its unique solution is given by

$$u(x) = x^3 - \frac{3}{2}x^2 + \frac{1}{2}. \tag{2.30}$$

Proof. First we must determine the operators B_1, A and A_0. By comparing Problem (2.29) with (2.14) it is natural to take $X = C[0,1]$,

$$B_1u = u'''(x) - 8x^2\int_0^1 tu'(t)dt - (3x+1)\int_0^1 t^2u'''(t)dt = 2x^2 - 6x + 4, \tag{2.31}$$

$$D(B_1) = \{u(x) \in C^3[0,1] : u(0) = 2\int_0^1 u(t)dt, \quad u'(0) = -u'(1),\ u''(0) = -u''(1)\},$$

$$\Phi(A_0u) = \int_0^1\int_0^1 tu'(t)dtdy,\ F(AA_0u) = \int_0^1\int_0^1 t^2u'''(t)dtdy, \tag{2.32}$$
$$\mathcal{A}x = AA_0u(x) = u'''(x), \quad A_0u = u'(x).$$

Denote $v(x) = u'(x)$. Then $AA_0u(x) = u'''(x) = (u'(x))'' = Av(x) = v''(x)$. From boundary conditions (2.31) follws that $v(0) = u'(0) = -u'(1) = -v(1)$, $v'(0) = u''(0) = -u''(1) = -v'(1)$. So the operators A, A_0 are defined by

$$Av(x) = v''(x), \quad D(A) = \{v(x) \in C^2[0,1] :\ v(0) = -v(1),\ v'(0) = -v'(1)\},$$

$$A_0u(x) = u'(x), \quad D(A_0) = \{u(x) \in C^1[0,1] :\ u(0) = 2\int_0^1 u(x)dx\}.$$

Now we make sure that $D(B_1) = D(AA_0)$. Using the definition of the product operators we get

$$D(AA_0) = \{u(x) \in D(A_0) : A_0u \in D(A)\} = \{u(x) \in C^1[0,1] : u(0) =$$
$$= 2\int_0^1 u(x)dx,\ u'(x) \in C^2[0,1],\ u'(0) = -u'(1),\ u''(0) = -u''(1)\} = D(B_1).$$

Since $D(B_1) = D(AA_0)$, we can apply Theorem 2.3. It is easy to verify that the operators A and A_0 are correct and their inverse operators for all $f(t) \in C[0,1]$ are given by

$$A_0^{-1} f(x) = 2\int_0^1 (t-1) f(t)dt + \int_0^x f(t)dt, \tag{2.33}$$

$$A^{-1} f(x) = \tfrac{1}{2}\int_0^1 \left(t - x - \tfrac{1}{2}\right) f(t)dt + \int_0^x (x-t) f(t)dt. \tag{2.34}$$

By comparing again (2.31) with (2.14) it is natural to take $S = S(x) = 8x^2$, $G = G(x) = 3x+1$. From (2.32) we get

$$\Phi(f) = \int_0^1 t f(t)dt, \quad F(f) = \int_0^1 t^2 f(t)dt. \tag{2.35}$$

Let $\hat{f}(x) = A^{-1} f(x)$ and $AA_0 u(x) = f(x)$. Then, since A_0, A are invertible, by means of (2.33) and (2.34) we have

$$\begin{aligned} u(x) &= A_0^{-1} A^{-1} f(x) = A_0^{-1} \hat{f}(x) = 2\int_0^1 (t-1)\hat{f}(t)dt + \int_0^x \hat{f}(t)dt = \\ &= 2\int_0^1 (t-1)\left[\tfrac{1}{2}\int_0^1 \left(s - t - \tfrac{1}{2}\right) f(s)ds + \int_0^t (t-s) f(s)ds\right] dt + \\ &+ \int_0^x \left[\tfrac{1}{2}\int_0^1 \left(s - t - \tfrac{1}{2}\right) f(s)ds + \int_0^t (t-s) f(s)ds\right] dt. \end{aligned}$$

Further using Fubini theorem we obtain

$$\begin{aligned} A_0^{-1} A^{-1} f(x) &= -\tfrac{1}{12}\int_0^1 [3x^2 + 3x(1-2s) - 4s^3 + 12s^2 - 6s - 1] f(s)ds + \\ &+ \tfrac{1}{2}\int_0^x (x-s)^2 f(s)ds. \end{aligned} \tag{2.36}$$

Using (2.36) for $f = f(x) = 2x^2 - 6x + 4$ and $G = 3x + 1$ we get

$$\begin{aligned} A_0^{-1} A^{-1} f &= -\tfrac{1}{12}\int_0^1 [3x^2 + 3x(1-2s) - 4s^3 + 12s^2 - 6s - 1](2s^2 - 6s + 4)ds + \\ &+ \tfrac{1}{2}\int_0^x (x-s)^2 (2s^2 - 6s + 4)ds = \tfrac{1}{60}(2x^5 - 15x^4 + 40x^3 - 25x^2 - 10x + 12), \end{aligned} \tag{2.37}$$

$$\begin{aligned} A_0^{-1} A^{-1} &= -\tfrac{1}{12}\int_0^1 [3x^2 + 3x(1-2s) - 4s^3 + 12s^2 - 6s - 1](3s + 1)ds + \\ &+ \tfrac{1}{2}\int_0^x (x-s)^2 (3s + 1)ds = \tfrac{1}{120}(15x^4 + 20x^3 - 75x^2 + 15x + 19). \end{aligned} \tag{2.38}$$

Using (2.34) for $S = S(x) = 8x^2$, $G = G(x) = 3x + 1$, $\quad f(x) = 2x^2 - 6x + 4$ we find

$$\begin{aligned} A^{-1} S &= \tfrac{1}{2}\int_0^1 \left(t - x - \tfrac{1}{2}\right)(8t^2)dt + \int_0^x (x-t)(8t^2)dt = \tfrac{2x^4 - 4x + 1}{3}, \\ A^{-1} G &= \tfrac{1}{2}\int_0^1 \left(t - x - \tfrac{1}{2}\right)(3t + 1)dt + \int_0^x (x-t)(3t+1)dt = \tfrac{4x^2(x+1) - 10x + 1}{8}, \\ A^{-1} f &= \tfrac{1}{2}\int_0^1 \left(t - x - \tfrac{1}{2}\right)(2t^2 - 6t + 4)dt + \int_0^x (x-t)(2t^2 - 6t + 4)dt \\ &= \tfrac{x^2(x^2 - 6x + 12) - 5x - 1}{6}. \end{aligned}$$

Then by using (2.35) we arrive at

$$\begin{aligned} \Phi(A^{-1} G) &= \tfrac{1}{8}\int_0^1 t[4t^2(t+1) - 10t + 1]dt = -\tfrac{31}{240}, \\ F(G) &= \int_0^1 t^2(3t+1)dt = \tfrac{13}{12}, \\ \Phi(A^{-1} f) &= \tfrac{1}{6}\int_0^1 t[t^2(t^2 - 6t + 12) - 5t - 1]dt = -\tfrac{1}{30}, \\ F(f) &= \int_0^1 t^2(2t^2 - 6t + 4)dt = \tfrac{7}{30}, \quad F(S) = \int_0^1 t^2(8t^2)dt = \tfrac{8}{5}. \end{aligned}$$

Further by (2.17), (2.18) and (2.19) we find

$$\begin{aligned} \det L &= \det[I_m - F(G)] = 1 - 13/12 = -1/12, \\ G_0 &= G_0(x,y) = A^{-1} S + A^{-1} G L^{-1} F(S) = \tfrac{2x^4 - 4x + 1}{3} + \tfrac{4x^2(x+1) - 10x + 1}{8}(-12)\tfrac{8}{5} \\ &= \tfrac{10x^4 - 144x^3 - 144x^2 + 340x - 31}{15}, \\ \Phi(G_0) &= \tfrac{1}{15}\int_0^1 t(10t^4 - 144t^3 - 144t^2 + 340t - 31)dt = \tfrac{347}{150}, \\ \det L_0 &= \det[I_m - \Phi(G_0)] = 1 - \tfrac{347}{150} = -\tfrac{197}{150}. \end{aligned}$$

Since $\det L, \det L_0 \neq 0$, by Theorem 2.3, Problem (2.31) or (2.29) is correct. Applying (2.33) we thus have

$$\begin{aligned} A_0^{-1} G_0 &= 2\int_0^1 (t-1) G_0(t)dt + \int_0^x G_0(t)dt = \\ &= \tfrac{2}{15}\int_0^1 (t-1)(10t^4 - 144t^3 - 144t^2 + 340t - 31)dt + \end{aligned}$$

$$+\tfrac{1}{15}\int_0^x (10t^4-144t^3-144t^2+340t-31)dt =$$
$$= -\tfrac{223}{75}+\tfrac{x(2x^4-36x^3-48x^2+170x-31)}{15}.$$

Substituting the above values into (2.9) we get the solution (2.30). □

3. Factorization of hyperbolic integro-differential equations with integral boundary conditions

Everywhere below $\overline{\Omega}=\{(x,y)\in\mathbb{R}^2 : 0\leqslant x,y\leqslant 1\}$.

Lemma 3.1. *Let $a(x), c(x)\in C[0,1]$, $K(y)\in C[0,1]$. Then the operator $A: C(\bar{\Omega})\to C(\bar{\Omega})$ corresponding to the problem:*

$$Au(t)=u'_y(x,y)+c(x)u(x,y)=f(x,y), \tag{3.1}$$

$$D(A)=\Big\{u(x,y)\in C(\bar{\Omega}) : u'_y(x,y)\in C(\bar{\Omega}),\ u(x,0)=a(x)\int_0^1 K(y)u(x,y)dy\Big\}$$

is correct if and only if

$$a(x)\int_0^1 K(y)e^{-yc(x)}dy\neq 1, \tag{3.2}$$

and the unique solution of the above problem is given by the formula

$$u(x,y) = A^{-1}f(x,y)=a(x)e^{-yc(x)}\Big(1-a(x)\int_0^1 K(y)e^{-yc(x)}dy\Big)^{-1}\times$$
$$\times\int_0^1 K(y)e^{-yc(x)}\int_0^y f(x,t)e^{tc(x)}dtdy+e^{-yc(x)}\int_0^y f(x,t)e^{tc(x)}dt. \tag{3.3}$$

Proof. Assume that $u(x,y)\in\ker A$ and (3.2) hold. Then from (3.1) we get

$$u'_y(x,y)+c(x)u(x,y)=0,\quad u(x,0)=a(x)\int_0^1 K(y)u(x,y)dy. \tag{3.4}$$

From the above equation by integration on y we obtain

$$u(x,y)=u(x,0)e^{-yc(x)},\quad u(x,y)=a(x)e^{-yc(x)}\int_0^1 K(y)u(x,y)dy, \tag{3.5}$$
$$\int_0^1 K(y)u(x,y)dy=a(x)\int_0^1 K(y)e^{-yc(x)}dy\int_0^1 K(y)u(x,y)dy,$$
$$\Big[1-a(x)\int_0^1 K(y)e^{-yc(x)}dy\Big]\int_0^1 K(y)u(x,y)dy=0.$$

From the last equation, since (3.2), follows that $\int_0^1 K(y)u(x,y)dy=0$. Substitution of this value into (3.5) implies $u(x,y)=0$. This means that the operator A is injective.

Conversaly. Let $u(x,y)\in\ker A$ and $a(x)\int_0^1 K(y)e^{-yc(x)}dy=1$. Then (3.4) holds. It is easy to verify that $u(x,y)=e^{-yc(x)}$ satisfies problem (3.4). Thus we prove that $u(x,y)=e^{-yc(x)}\in\ker A$ and so A is not injective.

We will find the solution to (3.1). Let $a(x)\int_0^1 K(y)e^{-yc(x)}dy\neq 1$. Then A is injective and problem (3.1) has a unique solution. From (3.1) by integration on y we obtain

$$u(x,y) = e^{-yc(x)}a(x)\int_0^1 K(y)u(x,y)dy+e^{-yc(x)}\int_0^y f(x,t)e^{tc(x)}dt, \tag{3.6}$$
$$\int_0^1 K(y)u(x,y)dy=a(x)\int_0^1 K(y)e^{-yc(x)}dy\int_0^1 K(y)u(x,y)dy+$$
$$+\int_0^1 K(y)e^{-yc(x)}\int_0^y f(x,t)e^{tc(x)}dtdy,$$
$$\Big[1-a(x)\int_0^1 K(y)e^{-yc(x)}dy\Big]\int_0^1 K(y)u(x,y)dy=$$
$$=\int_0^1 K(y)e^{-yc(x)}\int_0^y f(x,t)e^{tc(x)}dtdy.$$

Then since (3.2) we obtain

$$\int_0^1 K(y)u(x,y)dy = \Big(1-a(x)\int_0^1 K(y)e^{-yc(x)}dy\Big)^{-1}\times$$
$$\times\int_0^1 K(y)e^{-yc(x)}\int_0^y f(x,t)e^{tc(x)}dtdy. \tag{3.7}$$

Substituting (3.7) into (3.6), we obtain the unique solution (3.3) to (3.1) for every $f \in C(\bar{\Omega})$. Since f in (3.3) is an arbitrary element of $C(\bar{\Omega})$, then $R(A) = C(\bar{\Omega})$. It is easy to verify that A^{-1} is bounded. Hence A is correct. □

Lemma 3.2. *Let $b(y), d(y) \in C[0,1]$, $K_0(x) \in C[0,1]$. Then the operator $A_0 : C(\bar{\Omega}) \to C(\bar{\Omega})$ corresponding to the problem:*

$$A_0 u(t) = u'_x(x,y) + d(y)u(x,y) = f(x,y), \tag{3.8}$$
$$D(A_0) = \left\{ u(x,y) \in C(\bar{\Omega}) : u'_x \in C(\bar{\Omega}),\ u(0,y) = b(y) \int_0^1 K_0(x)u(x,y)dx \right\}$$

is correct if and only if

$$b(y) \int_0^1 K_0(x) e^{-xd(y)} dx \neq 1 \tag{3.9}$$

and the unique solution of the above problem is given by the formula

$$\begin{aligned} u(x,y) \quad &= A_0^{-1} f(x,y) = b(y) e^{-xd(y)} \left(1 - b(y) \int_0^1 K_0(x) e^{-xd(y)} dx\right)^{-1} \times \\ &\times \int_0^1 K_0(x) e^{-xd(y)} \int_0^x f(s,y) e^{sd(y)} ds dx + e^{-xd(y)} \int_0^x f(s,y) e^{sd(y)} ds. \end{aligned} \tag{3.10}$$

Proof. Assume that $u(x,y) \in \ker A_0$ and (3.9) hold. Then from (3.8) we get

$$u'_x(x,y) + d(y)u(x,y) = 0, \quad u(0,y) = b(y) \int_0^1 K_0(x)u(x,y)dx. \tag{3.11}$$

From the last equation by integration on x we obtain

$$u(x,y) = u(0,y)e^{-xd(y)}, \quad u(x,y) = e^{-xd(y)} b(y) \int_0^1 K_0(x)u(x,y)dx, \tag{3.12}$$
$$\int_0^1 K_0(x)u(x,y)dx = b(y) \int_0^1 K_0(x) e^{-xd(y)} dx \int_0^1 K_0(x)u(x,y)dx,$$
$$\left[1 - b(y) \int_0^1 K_0(x) e^{-xd(y)} dx\right] \int_0^1 K_0(x)u(x,y)dx = 0.$$

If $b(y) \int_0^1 K_0(x) e^{-xd(y)} dx \neq 1$, we get $\int_0^1 K_0(x)u(x,y)dx = 0$. Substitution of this value into (3.12) implies $u(x,y) = 0$. This means that A_0 is injective.

Conversaly. Let $u(x,y) \in \ker A_0$ and $b(y) \int_0^1 K_0(x) e^{-xd(y)} dx = 1$. Then (3.11) holds. It is easy to verify that $u(x,y) = e^{-xd(y)} \neq 0$ satisfies (3.11). Thus we prove that $\ker A_0 \neq \{0\}$ and so A_0 is not injective.

We will find the solution to (3.8). Let $b(y) \int_0^1 K_0(x) e^{-xd(y)} dx \neq \pm 1$. Then A_0 is injective and Problem (3.8) has a unique solution. From (3.8) by integration on x for every $f \in C(\bar{\Omega})$ we obtain

$$u(x,y) \quad = e^{-xd(y)} b(y) \int_0^1 K_0(x)u(x,y)dx + e^{-xd(y)} \int_0^x f(s,y) e^{sd(y)} ds, \tag{3.13}$$
$$\int_0^1 K_0(x)u(x,y)dx = b(y) \int_0^1 K_0(x) e^{-xd(y)} dx \int_0^1 K_0(x)u(x,y)dx +$$
$$+ \int_0^1 K_0(x) e^{-xd(y)} \int_0^x f(s,y) e^{sd(y)} ds dx,$$
$$\left[1 - b(y) \int_0^1 K_0(x) e^{-xd(y)} dx\right] \int_0^1 K_0(x)u(x,y)dx =$$
$$= \int_0^1 K_0(x) e^{-xd(y)} \int_0^x f(s,y) e^{sd(y)} ds dx.$$

Then since (3.9) we obtain

$$\begin{aligned} \int_0^1 K_0(x)u(x,y)dx \quad &= \left(1 - b(y) \int_0^1 K_0(x) e^{-xd(y)} dx\right)^{-1} \times \\ &\times \int_0^1 K_0(x) e^{-xd(y)} \int_0^x f(s,y) e^{sd(y)} ds dx. \end{aligned} \tag{3.14}$$

Substituting (3.14) into (3.13), we obtain the unique solution (3.10) to (3.8) for every $f \in C(\bar{\Omega})$. Since f in (3.10) is an arbitrary element of $C(\bar{\Omega})$, then $R(A_0) = C(\bar{\Omega})$. It is easy to verify that A_0^{-1} is bounded. Hence A_0 is correct. □

Theorem 3.3. *Let $a(x), c(x), K_0(x) \in C[0,1]$, $b(y), K(y) \in C[0,1], d(y) \in C^1[0,1]$, $h(x,y), u(x,y) \in C^1(\bar{\Omega})$, $u''_{xy}(x,y) \in C(\bar{\Omega})$. Then the problem*

$$u''_{xy}(x,y) + c(x)u_x(x,y) + d(y)u'_y(x,y) + h(x,y)u(x,y) = f(x,y), \tag{3.15}$$
$$u(0,y) = b(y) \int_0^1 K_0(x)u(x,y)dx,$$
$$u'_x(x,0) + d(0)u(x,0) = a(x) \int_0^1 K(y)[u'_x(x,y) + d(y)u(x,y)]dy$$

is correct if

$$h(x,y) = d'(y) + c(x)d(y), \tag{3.16}$$

$$a(x)\int_0^1 K(y)e^{-yc(x)}dy \neq 1, \quad b(y)\int_0^1 K_0(x)e^{-xd(y)}dx \neq 1 \tag{3.17}$$

and its unique solution is given by the formula

$$u(x,y) = b(y)e^{-xd(y)}\left(1 - b(y)\int_0^1 K_0(x)e^{-xd(y)}dx\right)^{-1} \times \tag{3.18}$$
$$\times \int_0^1 K_0(x)e^{-xd(y)}\int_0^x v(s,y)e^{sd(y)}dsdx + e^{-xd(y)}\int_0^x v(s,y)e^{sd(y)}ds,$$

where

$$v(x,y) = a(x)e^{-yc(x)}\left(1 - a(x)\int_0^1 K(y)e^{-yc(x)}dy\right)^{-1} \times \tag{3.19}$$
$$\times \int_0^1 K(y)e^{-yc(x)}\int_0^y f(x,t)e^{tc(x)}dtdy + e^{-yc(x)}\int_0^y f(x,t)e^{tc(x)}dt.$$

Proof. Let the operator A be defined by (3.1) and the operator A_0 by (3.8), where we suppose that $d(y) \in C^1[0,1]$. Denote by A_1 the operator corresponding to Problem (3.15), namely:

$$A_1u(x,y) = u''_{xy}(x,y) + c(x)u'_x(x,y) + d(y)u'_y(x,y) + h(x,y)u(x,y), \tag{3.20}$$

$$D(A_1) = \{u(x,y) \in C(\bar{\Omega}) : u'_x(x,y), u'_y(x,y), u''_{xy}(x,y) \in C(\bar{\Omega}), \tag{3.21}$$

$$u(0,y) = b(y)\int_0^1 K_0(x)u(x,y)dx,$$

$$u'_x(x,0) + d(0)u(x,0) = a(x)\int_0^1 K(y)[u'_x(x,y) + d(y)u(x,y)]dy\}.$$

We will prove that $A_1 = AA_0$, i.e. $D(A_1) = D(AA_0)$, $A_1u = AA_0u$ for all $u \in D(A_1)$ if $h(x,y) = d'(y) + c(x)d(y)$. Using the definition of a superposition of two operators, we find

$$D(AA_0) = \{u \in D(A_0) : A_0u \in D(A)\} = \tag{3.22}$$

$$= \{u(x,y) \in C(\bar{\Omega}) : u'_x \in C(\bar{\Omega}),\ u(0,y) = b(y)\int_0^1 K_0(x)u(x,y)dx,\ A_0u \in D(A)\} =$$

$$= \{u(x,y) \in C(\bar{\Omega}) : u'_x(x,y) \in C(\bar{\Omega}),\ (u'_x(x,y) + d(y)u(x,y))'_y \in C(\bar{\Omega}),$$

$$u(0,y) = b(y)\int_0^1 K_0(x)u(x,y)dx,$$

$$u'_x(x,0) + d(0)u(x,0) = a(x)\int_0^1 K(y)[u'_x(x,y) + d(y)u(x,y)]dy\},$$

$$AA_0u(x,y) = (u'_x(x,y) + d(y)u(x,y))'_y + c(x)[u'_x(x,y) + d(y)u(x,y)]. \tag{3.23}$$

Since $d(y) \in C^1[0,1]$, from $(u'_x(x,y) + d(y)u(x,y))'_y \in C(\bar{\Omega})$ follows that $u''_{xy} \in C(\bar{\Omega})$ and

$$(u'_x(x,y) + d(y)u(x,y))'_y = u''_{xy}(x,y) + d'(y)u(x,y) + d(y)u'_y(x,y) \in C(\bar{\Omega}).$$

Then from (3.22) follows that $D(AA_0) = D(A_1)$. Furthermore if the condition (3.16) is additionally satisfied then (3.23) implies $A_1u = AA_0u$ for all $u \in D(A_1)$. Thus we proved that if (3.16) holds, then $A_1 = AA_0$. Now we find the solvability condition and solution of $A_1u = f$, $u \in D(A_1)$ for the case when (3.16) holds. Denote by $v(x,y) = A_0u(x,y) = u'_x(x,y) + d(y)u(x,y)$. Then $A_1u = AA_0u = Av = f$. The last equation is correct by Lemma 3.1 if and only if (3.2) is satisfied. Then $v = A_0u = A^{-1}f$ where $A^{-1}f$ is calculated by (3.3) which is (3.19). The equation $A_0u = v$ is correct by Lemma 3.2 if and only if (3.9) is satisfied. Then $u = A_0^{-1}v$ where $A_0^{-1}v$ is calculated by (3.10) which is (3.18). Thus we proved that if (3.16), (3.17) hold true then the operator A_1 or Problem (3.15) is correct and its unique solution is (3.18) where $v(x,y)$ is given by (3.19). The theorem is proved. □

From Theorem 3.3 for $c(x) = d(y) = h(x,y) = 0$ follows the next

Corollary 3.4. *Let* $a(x), K_0(x) \in C[0,1]$, $b(y), K(y) \in C[0,1]$, $u(x,y) \in C^1(\bar{\Omega})$, $u''_{xy}(x,y) \in C(\bar{\Omega})$. *Then the problem*

$$u''_{xy}(x,y) = f(x,y), \tag{3.24}$$
$$u(0,y) = b(y)\int_0^1 K_0(x)u(x,y)dx,$$
$$u'_x(x,0) = a(x)\int_0^1 K(y)u'_x(x,y)dy$$

is correct on $C(\bar{\Omega})$ *if*

$$a(x)\int_0^1 K(y)dy \neq 1, \quad b(y)\int_0^1 K_0(x)dx \neq 1. \tag{3.25}$$

and the unique solution of Problem (3.24) is given by the formula

$$u(x,y) = \tag{3.26}$$
$$= \frac{b(y)}{1-b(y)\int_0^1 K_0(x)dx}\int_0^1 K_0(x)\left[\int_0^x \frac{a(s)}{1-a(s)\int_0^1 K(y)dy}\int_0^1 K(y)\int_0^y f(s,t)dtdyds + \right.$$
$$\left. + \int_0^x\int_0^y f(s,t)dtds\right]dx + \int_0^x \frac{a(s)}{1-a(s)\int_0^1 K(y)dy}\int_0^1 K(y)\int_0^y f(s,t)dtdyds +$$
$$+ \int_0^x\int_0^y f(s,t)dtds.$$

The following problem is solved by Theorem 2.3.

Example 3.5. Let $u(x,y), u'_x(x,y), u'_y(x,y), u''_{xy} \in C(\overline{\Omega})$. Then the problem

$$\begin{gathered} u''_{xy} \quad -(x+y)\int_0^1\int_0^1 xu'_x(x,y)dxdy - 3x^3\int_0^1\int_0^1 y^2u''_{xy}(x,y)dxdy \\ = 15x^3 - 2x - 2y, \\ u'_x(x,0) = 0, \quad u(0,y) = (y+1)\int_0^1 u(x,y)dx, \end{gathered} \tag{3.27}$$

is uniquelly solvable if $y \neq 0$ and the unique solution of (3.27) is given by the formula

$$u(x,y) = 5x^4y - y - 1. \tag{3.28}$$

Proof. Denote by B_1 the operator corresponding to Problem (3.27). First we must determine the operators A and A_0 and make sure that $D(B_1) = D(AA_0)$. Comparing (3.27) with (2.14) it is natural to take $X = C(\overline{\Omega})$,

$$\begin{gathered} \Phi(A_0u) = \int_0^1\int_0^1 xu'_x(x,y)dxdy, \quad F(AA_0u) = \int_0^1\int_0^1 y^2u''_{xy}(x,y)dxdy, \\ AA_0u(x,y) = u''_{xy}(x,y), \quad A_0u = u'_x(x,y). \end{gathered} \tag{3.29}$$

Denote $v(x,y) = u'_x(x,y)$. Then $AA_0u(x,y) = u''_{xy}(x,y) = (u'_x(x,y))'_y = Av(x,y) = v'_y(x,y)$. From boundary conditions (3.27) follws that $v(x,0) = 0$. So the operators A, A_0 are defined by

$$\begin{gathered} Av(x,y) = v'_y(x,y), \quad D(A) = \{v(x,y) \in C(\bar{\Omega}) : v'_y \in C(\bar{\Omega}),\, v(x,0) = 0\}, \\ A_0u(x,y) = u'_x(x,y), \quad D(A_0) = \big\{u(x,y) \in C(\bar{\Omega}) : u'_x \in C(\bar{\Omega}), \\ u(0,y) = (y+1)\int_0^1 u(x,y)dx\big\}. \end{gathered}$$

Then

$$\begin{gathered} D(AA_0) = \{u(x,y) \in D(A_0) : A_0u \in D(A)\} = \{u(x,y) \in C(\bar{\Omega}) : \\ u'_x, u''_{xy} \in C(\bar{\Omega}), \quad u(0,y) = (y+1)\int_0^1 u(x,y)dx,\, u'_x(x,0) = 0\} = D(B_1). \end{gathered}$$

Since $D(B_1) = D(AA_0)$, we can apply Theorem 2.3. Note that the operator A coincides with the operator A from Lemma 3.1 if $a(x) = c(x) = 0$ and the operator A_0 coincides with the operator A_0 from Lemma 3.2 if $b(y) = y+1$, $d(y) = 0$, $K_0(x) = 1$. Then by Lemma 3.1, the operator A is correct and

$$A^{-1}f(x,y) = \int_0^y f(x,t)dt, \tag{3.30}$$

by Lemma 3.2 the operator A_0 is correct if and only if $y \neq 0$ and its inverse is defined by

$$A_0^{-1}f(x,y) = -\frac{y+1}{y}\int_0^1 (1-s)f(s,y)ds + \int_0^x f(s,y)ds. \tag{3.31}$$

Notice that the operator AA_0 coincides with the operator corresponding to Problem (3.24) and, by Corollary 3.4, is correct if $y \neq 0$ and its inverse is defined by

$$A_0^{-1}A^{-1}f(x,y) = -\frac{y+1}{y}\int_0^1\int_0^x\int_0^y f(s,t)dtdsdx + \int_0^x\int_0^y f(s,t)dtds. \tag{3.32}$$

Comparing again (3.27) with (2.14) it is natural to take $S = x+y$, $G = 3x^3$, $f = 15x^3 - 2x - 2y$. From (3.29) follows that

$$\Phi(f) = \int_0^1\int_0^1 xf(x,y)dxdy, \quad F(f) = \int_0^1\int_0^1 y^2f(x,y)dxdy. \tag{3.33}$$

Using (3.32) for $f = 15x^3 - 2x - 2y$ and $G = 3x^3$ we find

$$A_0^{-1}A^{-1}f(x,y) = -\frac{y+1}{y}\int_0^1\int_0^x\int_0^y(15s^3-2s-2t)dtdsdx+$$
$$+\int_0^x\int_0^y(15s^3-2s-2t)dtds = \frac{45x^4y-12x^2y-12xy^2+(y+1)(6y-5)}{12},$$
$$A_0^{-1}A^{-1}G = -\frac{y+1}{y}\int_0^1\int_0^x\int_0^y 3s^3dtdsdx+$$
$$+\int_0^x\int_0^y 3s^3dtds = -\frac{3}{20}(y+1)+\frac{3}{4}x^4y+\frac{5x^4y+6x^2y+6xy^2-3(y+1)^2}{12}.$$

By means (3.30) for $G = 3x^3, \quad S = x+y$ we get

$$A^{-1}G = \int_0^y G(x,t)dt = \int_0^y 3x^3dt = 3x^3y,$$
$$A^{-1}S = \int_0^y S(x,t)dt = \int_0^y(x+t)dt = xy+y^2/2,$$
$$A^{-1}f = \int_0^y f(x,t)dt = \int_0^y(15x^3-2x-2y)dt = 15x^3y-2xy-y^2.$$

Using (3.33) we get

$$F(S) = \int_0^1\int_0^1 y^2S(x,y)dxdy = \int_0^1\int_0^1 y^2(x+y)dxdy = \frac{5}{12},$$
$$F(G) = \int_0^1\int_0^1 y^2G(x,y)dxdy = \int_0^1\int_0^1 y^23x^3dxdy = \frac{1}{4},$$
$$F(f) = \int_0^1\int_0^1 y^2f(x,y)dxdy = \int_0^1\int_0^1 y^2(15x^3-2x-2y)dxdy = \frac{5}{12},$$
$$\Phi(A^{-1}G) = \int_0^1\int_0^1 x3x^3ydxdy = \frac{3}{10},$$
$$\Phi(A^{-1}f) = \int_0^1\int_0^1 x(15x^3y-2xy-y^2)dxdy = 1.$$

Further by (2.17)-(2.19) we find

$$\begin{aligned} L &= I_m - F(G) = 1-1/4 = 3/4,\\ G_0 &= G_0(x,y) = A^{-1}S + A^{-1}GL^{-1}F(S) = xy+\frac{y^2}{2}+\frac{5}{3}x^3y,\\ L_0 &= I_m - \Phi(G_0) = 1-\int_0^1\int_0^1 xG_0(x,y)dxdy\\ &= 1-\int_0^1\int_0^1 x\left(xy+\frac{y^2}{2}+\frac{5}{3}x^3y\right)dxdy = \frac{7}{12}. \end{aligned}$$

Since $\det L = 3/4 \neq 0$ and $\det L_0 = 7/12 \neq 0$, by Theorem 2.3, Problem 3.27 is correct. Applying (3.31) obtain

$$\begin{aligned} A_0^{-1}G_0 &= -\frac{y+1}{y}\int_0^1(1-s)G_0(s,y)ds + \int_0^x G_0(s,y)ds\\ &= \frac{5x^4y+6x^2y+6xy^2-3(y+1)^2}{12}. \end{aligned}$$

Substituting the above values into (2.9) we get (3.28). □

References / Литература

[1] Adomian G. Solving Frontier Problems of Physics: The Decomposition Method. Massachusets: Kluwer Academic Publishers, 1994. DOI: https://doi.org/10.1007/978-94-015-8289-6.

[2] Barkovskii L.M., Furs A.N. Factorization of integro-differential equations of optics of dispersive anisotropic media and tensor integral operators of wave packet velocities. *Optics and Spectroscopy*, 2001, vol. 90, issue 4, pp. 561–567. DOI: http://doi.org/10.1134/1.1366751.

[3] Barkovskii L.M., Furs A.N. Factorization of integro-differential equations of the acoustics of dispersive viscoelastic anisotropic media and the tensor integral operators of wave packet velocities. *Acoustical Physics*, 2002, vol. 48, iss. 2, pp. 128–132. DOI: http://doi.org/10.1134/1.1460945.

[4] Caruntu D.I. Relied studies on factorization of the differential operator in the case of bending vibration of a class of beams with variable cross-section. *Revue Roumaine des Sci. Tech. Serie de Mecanique Appl.*, 1996, no. 41(5–6), pp. 389–397.

[5] Hirsa A., Neftci S.N. An Introduction to the Mathematics of Financial Derivatives. Cambridge: Academic Press, 2013. DOI: http://doi.org/10.1016/C2010-0-64929-7.

[6] Fahmy E.S. Travelling wave solutions for some time-delayed equations through factorizations. *Chaos Solitons & Fractals*, 2008, vol. 38, no. 4, pp. 1209–1216. DOI: http://dx.doi.org/10.1016/j.chaos.2007.02.007.

[7] Geiser J. Decomposition methods for differential equations: theory and applications. Boca Raton: CRC Press, Taylor and Francis Group, 2009, 304 p. DOI: https://doi.org/10.1201/9781439810972.

[8] Dong S.H. Factorization Method in Quantum Mechanics. *Fundamental Theories of Physics. Vol. 150.* Dordrecht: Springer, 2007, 308 p. Available at: https://777russia.ru/book/uploads/МЕХАНИКА/Dong%20S.-H.%20Factorization%20method%20in%20quantum%20mechanics%20%28Springer%2C%202007%29%28308s%29_PQm_.pdf.

[9] Nyashin Y., Lokhov V., Ziegler F. Decomposition method in linear elastic problems with eigenstrain. *Zamm Journa of applied mathematics and mechanics: Zeitschrift fur angewandte Mathematic and Mechanic*, 2005, vol. 85, no. 8, pp. 557–570. DOI: http://dx.doi.org/10.1002/zamm.200510202.

[10] C.V.M van der Mee. Semigroup and factorization methods in transport theory. (Mathematical Centre Tracts, 146). Mathematisch Centrum, Amsterdam, 1981. Available at: https://ir.cwi.nl/pub/13006/13006D.pdf.

[11] Berkovich L.M. Factorization as a method of finding of exact invariant solutions of the Kolmogorov-Petrovskii-Piskunov equation and related equations of Semenov and Zel'dovich. *Doklady Akademii Nauk*, 1992, vol. 322, no. 5, pp. 823–827. Available at: http://mi.mathnet.ru/eng/dan5636.

[12] Baskonus H.M., Bulut H., Pandir Y. The natural transform decomposition method for linear and nonlinear partial differential equations. *Mathematics in Engineering, Science and Aerospace*, 2014, vol. 5, no. 1, pp. 111–126. Available at: http://nonlinearstudies.com/index.php/mesa/article/view/823.

[13] Berkovich L.M. Method of factorization of ordinary differential operators and some of its applications. *Applicable Analysis and Discrete Mathematics*, 2007, vol. 1, no. 1, pp. 122–149. DOI: http://dx.doi.org/10.2298/AADM0701122B.

[14] Dehghan M. and Tatari M. Solution of a semilinear parabolic equation with an unknown control function using the decomposition procedure of Adomian. *Numerical Methods for Partial Differential Equations*, 2007, vol. 23, no. 3, pp. 499–510. DOI: http://dx.doi.org/10.1002/num.20186.

[15] El-Sayed S., Kaya D., Zarea S. The Decomposition Method Applied to Solve High-order Linear Volterra-Fredholm Integro-differential Equations. *International Journal of Nonlinear Sciences and Numerical Simulation*, 2004, vol. 5 (2), pp. 105–112. DOI: http://dx.doi.org/10.1515/IJNSNS.2004.5.2.105.

[16] Evans D.J., Raslan K.R. The Adomain decomposition method for solving delay differential equation. *International Journal of Computer Mathematics*, 2004, vol. 00, no. 1, pp. 1–6. DOI: http://dx.doi.org/10.1080/00207160412331286815.

[17] Hamoud A.A., Ghadle K.P. Modified Adomian Decomposition Method for Solving Fuzzy Volterra-Fredholm Integral Equation. *Journal of the Indian Mathematical Society*, 2018, vol. 85, no. 1–2, pp. 52–69. DOI: http://dx.doi.org/10.18311/jims/2018/16260.

[18] Rawashdeh M.S., Maitama S. Solving coupled system of nonliear PDEs using the natural decomposition method. *International Journal of Pure and Applied Mathematics*, 2014, vol. 92, no. 5, pp. 757–776. DOI: http://dx.doi.org/10.12732/ijpam.v92i5.10.

[19] Yang C., Hou J. Numerical solution of integro-differential equations of fractional order by Laplace decomposition method. *WSEAS Transactions on Mathematics*, 2013, vol. 12, no. 12, pp. 1173–1183. Available at: https://wseas.org/multimedia/journals/mathematics/2013/b105706-249.pdf.

[20] Wazwaz A.M. The combined Laplace transform-Adomian decomposition method for handling nonlinear Volterra integro-differential equations. *Applied Mathematics and Computation*, 2010, vol. 216, no. 4, pp. 1304–1309. DOI: http://dx.doi.org/10.1016/j.amc.2010.02.023.

[21] Assanova A.T. Nonlocal problem with integral conditions for the system of hyperbolic equations in the characteristic rectangle. *Russian Math.*, 2017, vol. 61, no. 5, pp. 7–20. DOI: http://dx.doi.org/10.3103/S1066369X17050024.

[22] Kozhanov A.I., Pul'kina L.S. On the Solvability of Boundary Value Problems with a Nonlocal Boundary Condition of Integral Form for Multidimentional Hyperbolic Equations. *Differential Equations*, 2006, vol. 42, no. 9, pp. 1233–1246. DOI: https://doi.org/10.1134/S0012266106090023.

[23] Ludmila S. Pulkina. Nonlocal Problems for Hyperbolic Equation from the Viewpoint of Strongly Regular Boundary Conditions. *Electronic Journal of Differential Equations*, 2020, no. 28, pp. 1–20. Available at: https://ejde.math.txstate.edu/.

[24] Pul'kina L.S. Initial-Boundary Value Problem with a Nonlocal Boundary Condition for a Multidimensional Hyperbolic Equation. *Differential Equations*, 2008, vol. 44, no. 8, pp. 1119–1125. DOI: http://dx.doi.org/10.1134/S0012266108080090.

[25] Pul'kina L.S. Boundary value problems for a hyperbolic equation with nonlocal conditions of the I and II kind. *Russian Mathematics*, 2012, vol. 56, no. 4, pp. 62–69. DOI: http://dx.doi.org/10.3103/S1066369X12040081.

[26] Parasidis I.N., Providas E., Tsekrekos P.C. Factorization of linear operators and some eigenvalue problems of special operators. *Bulletin of Bashkir University*, 2012, vol. 17, no. 2, pp. 830–839. Available at: https://cyberleninka.ru/article/n/factorization-of-linear-operators-and-some-eigenvalue-problems-of-special-operators/viewer; https://elibrary.ru/item.asp?id=17960431.

[27] Parasidis I.N., Providas E., Zaoutsos S. On the Solution of Boundary Value Problems for Ordinary Differential Equations of Order n and $2n$ with General Boundary Conditions. In: Daras N., Rassias T. (eds) Computational Mathematics and Variational Analysis. Springer Optimization and Its Applications, vol. 159. Springer, Cham, pp. 299–314. DOI: http://dx.doi.org/10.1007/978-3-030-44625-3_17.

[28] Vassiliev N.N., Parasidis I.N., Providas E. Exact solution method for Fredholm integro-differential equations with multipoint and integral boundary conditions. Part 2. Decomposition-extension method for squared operators. *Information and Control Systems*, 2019, issue 2, pp. 2—9. DOI: https://doi.org/10.31799/1684-8853-2019-2-2-9.

[29] Providas E., I.N. Parasidis On the solution of some higher-order integro-differential equations of special form. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2020, vol. 26, no. 1, pp. 14–22. DOI: http://doi.org/10.18287/2541-7525-2020-26-1-14-22.

[30] Parassidis I.N., Tsekrekos P.C. Some quadratic correct extensions of minimal operators in Banach space. *Operators and Matrices*, 2010, vol. 4, no. 2, pp. 225–243. DOI: http://dx.doi.org/10.7153/oam-04-11.

[31] Parasidis I.N. Extension and decomposition methods for differential and integro-differential equations. *Eurasian Mathematical Journal*, 2019, vol. 10, no. 3, pp. 48–67. DOI: https://doi.org/10.32523/2077-9879-2019-10-3-48-67.

Научная статья

DOI: 10.18287/2541-7525-2021-27-1-29-43

УДК 629

Дата: поступления статьи: 15.01.2021
после рецензирования: 17.02.2021
принятия статьи: 28.02.2021

Е. Провидас
Университет Фессалии, г. Ларисса, Греция
E-mail: providas@uth.gr. ORCID: https://orcid.org/0000-0002-0675-4351
Л.С. Пулькина
Самарский национальный исследовательский университет
имени академика С.П. Королева, г. Самара, Российская Федерация
E-mail: louise@samdiff.ru. ORCID: https://orcid.org/0000-0001-7947-612
И.Н. Парасидис
Университет Фессалии, г. Ларисса, Греция
E-mail: paras@teilar.gr. ORCID: https://orcid.org/0000-0002-7900-9256

ФАКТОРИЗАЦИЯ ОБЫКНОВЕННЫХ И ГИПЕРБОЛИЧЕСКИХ ИНТЕГРО-ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ С ИНТЕГРАЛЬНЫМИ УСЛОВИЯМИ В БАНАХОВОМ ПРОСТРАНСТВЕ

АННОТАЦИЯ

В статье исследованы условия существования единственного точного решения для одного класса абстрактных операторных уравнений вида $B_1u = \mathcal{A}u - S\Phi(A_0u) - GF(\mathcal{A}u) = f, \quad u \in D(B_1)$, где $\mathcal{A}, A_0$ — линейные абстрактные операторы; G, S — линейные векторы; Φ, F — линейные функциональные векторы. Этот класс уравнений полезен для решения краевых задач для интегро-дифференциальных уравнений в случае, когда $\mathcal{A}, A_0$ — дифференциальные операторы, а $F(\mathcal{A}u)$, $\Phi(A_0u)$ — интегральные операторы Фредгольма. Показано, что операторы типа B_1 могут быть в некоторых случаях представлены как произведения двух более простых операторов B_G, B_{G_0} специального вида, что позволяет получить условие существования единственного точного решения уравнения $B_1u = f$ из условий однозначной разрешимости уравнений $B_Gv = f$ и $B_{G_0}u = v$.

Ключевые слова: корректная (по Адамару) разрешимость; метод факторизации (декомпозиции); интегро-дифференциальные уравнения Фредгольма; начальная задача; нелокальная краевая задача с интегральными условиями.

Цитирование. Providas E., Pulkina L.S., Parasidis I.N. Factorization of ordinary and hyperbolic integro-differential equations with integral boundary conditions in a Banach space // Вестник Самарского университета. Естественнонаучная серия. 2021. Т. 27, № 1. С. 29–43. DOI: http://doi.org/10.18287/2541-7525-2021-27-1-29–43.

Информация о конфликте интересов: авторы и рецензенты заявляют об отсутствии конфликта интересов.

© Провидас Е., 2021
Евтимиос Провидас — кандидат технических наук, доцент, Университет Фессалии, Греция, г. Ларисса, Гайополис, 41110.

© Пулькина Л.С., 2021
Людмила Степановна Пулькина — доктор физико-математических наук, профессор кафедры дифференциальных уравнений и теории управления, Самарский национальный исследовательский университет имени академика С.П. Королева, 443086, Российская Федерация, г. Самара, Московское шоссе, 34.

© Парасидис И.Н., 2021
Иван Нестерович Парасидис — кандидат технических наук, доцент, Университет Фессалии, Греция, г. Ларисса, Гайополис, 41110.

Научная статья
DOI: 10.18287/2541-7525-2021-27-1-44-61

УДК 512.531; 519.7

Дата: поступления статьи: 10.01.2021
после рецензирования: 17.02.2021
принятия статьи: 28.02.2021

С.М. Рацеев
Ульяновский государственный университет,
г. Ульяновск, Российская Федерация
E-mail: ratseevsm@mail.ru. ORCID: https://orcid.org/0000-0003-4995-9418
А.Д. Лавриненко
Ульяновский государственный университет,
г. Ульяновск, Российская Федерация
E-mail: anutalavrinenko@gmail.com. ORCID: https://orcid.org/0000-0003-3652-1097
Е.А. Степанова
Ульяновский государственный университет,
г. Ульяновск, Российская Федерация
E-mail: kate_stepanova@bk.ru. ORCID: https://orcid.org/0000-0003-0276-1615

ОБ АЛГОРИТМЕ БЕРЛЕКЭМПА — МЕССИ И ЕГО ПРИМЕНЕНИИ В АЛГОРИТМАХ ДЕКОДИРОВАНИЯ

АННОТАЦИЯ

В работе содержатся описание алгоритма Берлекэмпа — Месси и его эквивалентный вариант на основе обобщенного алгоритма Евклида. Также приводится оптимизированный алгоритм Берлекэмпа — Месси для случая поля характеристики два. Алгоритм Берлекэмпа — Месси имеет квадратичную сложность и применяется, например, для решения систем линейных уравнений, у которых матрица системы является матрицей Тёплица. В частности, такие системы уравнений появляются в алгоритмах синдромного декодирования кодов БЧХ, кодов Рида — Соломона, обобщенных кодов Рида — Соломона, кодов Гоппы. Приводятся алгоритмы декодирования перечисленных кодов на основе алгоритма Берлекэмпа — Месси.

Ключевые слова: алгоритм Берлекэмпа — Месси; обобщенный алгоритм Евклида; код Рида — Соломона; декодирование кода.

Цитирование. Рацеев С.М., Лавриненко А.Д., Степанова Е.А. Об алгоритме Берлекэмпа — Месси и его применении в алгоритмах декодирования // Вестник Самарского университета. Естественнонаучная серия. 2021. Т. 27, № 1. С. 44–61. DOI: http://doi.org/10.18287/2541-7525-2021-27-1-44-61.

Информация о конфликте интересов: авторы и рецензенты заявляют об отсутствии конфликта интересов.

© Рацеев С.М., 2021
Сергей Михайлович Рацеев — доктор физико-математических наук, доцент, профессор кафедры информационной безопасности и теории управления, Ульяновский государственный университет, 432017, Российская Федерация, г. Ульяновск, ул. Льва Толстого, 42.
© Лавриненко А.Д., 2021
Анна Дмитриевна Лавриненко — студент кафедры информационной безопасности и теории управления, Ульяновский государственный университет, 432017, Российская Федерация, г. Ульяновск, ул. Льва Толстого, 42.
© Степанова Е.А., 2021
Екатерина Алексеевна Степанова — студент кафедры информационной безопасности и теории управления, Ульяновский государственный университет, 432017, Российская Федерация, г. Ульяновск, ул. Льва Толстого, 42.

Введение

В технике один из наиболее распространенных методов генерации битовых последовательностей реализуется с помощью регистров сдвига с обратной линейной связью (Linear Feedback Shift Register – LFSR). Регистр сдвига с обратной связью (LFSR) — это регистр, который можно рассматривать как множество ячеек памяти, в каждой из которых записан один бит информации. На каждом шаге содержимое нескольких заранее определенных ячеек (отводов) пропускается через функцию обратной связи. Значение функции записывается в самую левую ячейку регистра, сдвигая все остальные его биты на одну позицию вправо. Выходом регистра на текущем шаге является «вытолкнутый» справа бит (рис. 1).

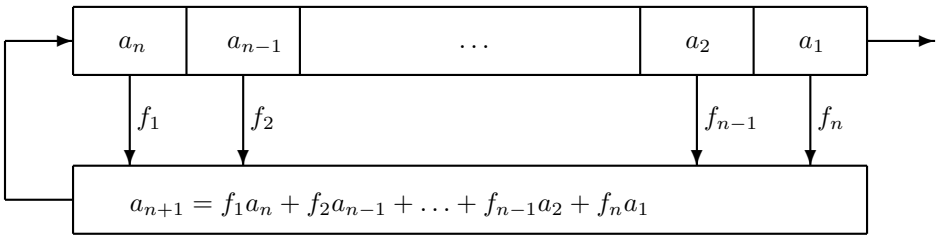

Рис. 1. Регистр сдвига с обратной связью
Fig. 1. Feedback shift register

Рассмотрим систему линейных уравнений над некоторым полем F относительно неизвестных $f_1, \ldots, f_n$:

$$\begin{pmatrix} a_n & a_{n-1} & \ldots & a_2 & a_1 \\ a_{n+1} & a_n & \ldots & a_3 & a_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{2n-1} & a_{2n-2} & \ldots & a_{n+1} & a_n \end{pmatrix} \begin{pmatrix} f_1 \\ f_2 \\ \ldots \\ f_n \end{pmatrix} = \begin{pmatrix} -a_{n+1} \\ -a_{n+2} \\ \ldots \\ -a_{2n} \end{pmatrix}. \tag{1}$$

У матрицы данной системы все диагонали, параллельные главной, имеют одинаковые элементы. Матрица такого вида называется диагонально-постоянной матрицей, или матрицей Тёплица. Решение данной системы уравнений методом Гаусса имеет сложность вычислений порядка n^3. Такие системы практичнее решать с помощью алгоритма Берлекэмпа — Месси, который дает сложность вычислений порядка n^2.

Алгебраические алгоритмы декодирования кодов БЧХ (в частности, кодов Рида — Соломона) можно разделить на два класса: синдромные и бессиндромные. Хорошо известные алгоритмы синдромного декодирования построены на основе алгоритма Питерсона — Горенстейна — Цирлера, алгоритма Берлекэмпа — Месси, алгоритма Сугиямы [1; 2]. К алгоритмам безсиндромного декодирования относится, например, алгоритм Гао [3]. Процесс синдромного декодирования можно разбить на четыре шага: 1) вычисление компонентов синдромного вектора на основе полученного вектора; 2) нахождение многочлена локаторов ошибок $\sigma(x)$, который содержит информацию о позициях ошибок; 3) нахождение корней многочлена $\sigma(x)$, по которым определяются позиции ошибок; 4) нахождение значений ошибок (для недвоичных кодов).

Второй этап декодирования является самым сложным. Многочлен локаторов ошибок $\sigma(x)$ можно найти несколькими способами. Один из первых способов нахождения $\sigma(x)$ — алгоритм Питерсона для двоичных кодов (на основе тождеств Ньютона) и Горенстейна — Цирлера для недвоичных кодов, который сводит данную задачу к решению системы из t линейных уравнений (например, с помощью метода Гаусса), где t — максимальное число ошибок, исправляемое кодом. Сложность такого декодирования пропорциональна t^3. Берлекэмп, используя особенности матрицы коэффициентов системы уравнений, уменьшил сложность нахождения многочлена $\sigma(x)$ до величины порядка t^2. Месси сумел интерпретировать алгоритм Берлекэмпа как алгоритм построения рекуррентного фильтра, тем самым упростив и понимание алгоритма, и его реализацию. В окончательном виде этот алгоритм получил название алгоритма Берлекэмпа — Месси.

Приведенные в данной работе алгоритмы декодирования позволяют исправлять не только ошибки, но и ошибки и стирания одновременно, поэтому они являются обобщением случая только ошибок. Поскольку авторы данной работы не нашли аналогов алгоритмов в других работах, то, вероятно, некоторые из них являются новыми. Все эти алгоритмы снабжены строгими математическими доказательствами.

1. Алгоритм Берлекэмпа — Месси

Лучшим подходом к алгоритму Берлекэмпа — Месси является интерпретация матричного уравнения (1) как описания рекурсивного фильтра. Предположим, что вектор $f = (f_1, \ldots, f_n)$ известен. Последовательность $a_1, a_2, \ldots$ в этом случае называется линейной рекуррентной последовательностью, члены которой вычисляются с помощью уравнения

$$a_j = -\sum_{i=1}^{n} f_i a_{j-i}, \quad j = n+1, n+2, \ldots$$

Изначально на элементы последовательности $a_1, a_2, \ldots$ каких-либо ограничений не накладывается. Произвольный LFSR можно задать многочленом $f(x)$ обратных связей $f(x) = 1 + f_1 x + \ldots + f_n x^n$ и длиной L регистра. Заметим, что длина регистра может быть больше степени многочлена $f(x)$, так как самые правые ячейки могут не включаться в обратную связь.

Для построения регистра сдвига нужно определить две величины: длину L регистра и многочлен $f(x)$ обратных связей при условии $\deg f(x) \leqslant L$. Обозначим эту пару через $(L, f(x))$. Данный LFSR должен порождать заданную последовательность $a_1, a_2, \ldots, a_{2n}$ и иметь минимальную длину L.

Основная идея алгоритма Берлекэмпа — Месси состоит в следующем. Алгоритм построения LFSR минимальной длины является рекурсивным. Для каждого $r = 2, 3, \ldots, 2n$ он строит LFSR, порождающий последовательность $a_1, \ldots, a_r$. LFSR минимальной длины, порождающий последовательность $a_1, \ldots, a_r$, обозначим через $(L_r, f^{(r)}(x))$. Такой регистр не обязательно должен определяться однозначно, так как возможно существование нескольких LFSR минимальной длины. К началу r-го шага имеется совокупность LFSR:

$$(L_1, f^{(1)}(x)),\ (L_2, f^{(2)}(x)), \ldots, (L_{r-1}, f^{(r-1)}(x)).$$

Алгоритм Берлекэмпа — Месси вычисляет новый LFSR $(L_r, f^{(r)}(x))$ минимальной длины, генерирующий последовательность $a_1, \ldots, a_r$. Для этого используется самый последний из вычисленных LFSR, в котором, при необходимости, модифицируются длина и весовые множители в отводах. На r-м шаге алгоритма вычисляется элемент с номером r на выходе $(r-1)$-го регистра сдвига:

$$\widetilde{a}_r = -\sum_{i=1}^{L_{r-1}} f_i^{(r-1)} a_{r-i}.$$

Если $\Delta_r = 0$, то полагаем $(L_r, f^{(r)}(x)) = (L_{r-1}, f^{(r-1)}(x))$ и завершаем этим самым r-й шаг алгоритма. Если $\Delta_r \neq 0$, то изменим весовые множители в LFSR по правилу

$$f^{(r)}(x) = f^{(r-1)}(x) + \left(-\frac{\Delta_r}{\Delta_m}\right) x^{r-m} f^{(m-1)}(x),$$

где число m удовлетворяет условию $L_{r-1} = L_{r-2} = \ldots = L_m > L_{m-1}$.

Теорема 1 [4]. Пусть $\left\{(L_r, f^{(r)}(x))\right\}_{r=1}^{n}$ — последовательность LFSR минимальной длины, таких, что $(L_r, f^{(r)}(x))$ генерирует последовательность $a_1, \ldots, a_r$. Если для некоторого r, $2 \leqslant r \leqslant n$, выполнено $f^{(r-1)}(x) \neq f^{(r)}(x)$, то

$$L_r = \max\{L_{r-1}, r - L_{r-1}\}.$$

Замечание 1. Пусть для некоторого r выполнено неравенство $f^{(r-1)}(x) \neq f^{(r)}(x)$. Тогда возможны два случая.

1. $L_r > L_{r-1}$. Тогда из теоремы 1 следует, что $L_r = r - L_{r-1} > L_{r-1}$. Поэтому $2L_{r-1} < r$.
2. $L_r = L_{r-1}$. Тогда $L_{r-1} \geqslant r - L_{r-1}$. Поэтому $2L_{r-1} \geqslant r$.

Учтем данное замечание при описании алгоритма Берлекэмпа — Месси. В следующем алгоритме многочлен $f(x)$ отвечает за многочлен LFSR $(L_r, f^{(r)}(x))$, а многочлен $b(x)$ — за многочлен LFSR $(L_{m-1}, f^{(m-1)}(x))$.

Алгоритм 1. (алгоритм Берлекэмпа — Месси).
Вход: последовательность $a_1, \ldots, a_n$ над некоторым полем F.
Выход: LFSR $(L, f(x))$ минимальной длины L, для которого

$$-a_j = \sum_{i=1}^{L} f_i a_{j-i}, \quad j = L+1,\ L+2, \ldots, n. \tag{2}$$

1. Определить $r := 0,\ f(x) := 1,\ b(x) := 1,\ L := 0.$

2. Цикл $r := 1, \ldots, n$:
   2.1. Определить $\Delta := a_r + \sum\limits_{i=1}^{L} f_i a_{r-i}$;
   2.2. Если $\Delta = 0$, то $b(x) := x \cdot b(x)$;
   2.3. Если $\Delta \neq 0$:
      2.3.1 $buf(x) := f(x) - \Delta \cdot x \cdot b(x)$;
      2.3.2. Если $2L < r$:
         $b(x) := \Delta^{-1} \cdot f(x)$,
         $f(x) := buf(x)$,
         $L := r - L$;
      2.3.3. Иначе (т. е. выполнено $2L \geqslant r$):
         $f(x) := buf(x)$,
         $b(x) := x \cdot b(x)$.

Заметим, что в алгоритме 1 можно минимизировать число вычислений обратных элементов в поле F, т. е. вычислений вида Δ^{-1}. Для этого стоит лишь заметить, что если для некоторого унитарного многочлена $f(x)$ выполнено равенство $a_r + \sum\limits_{i=1}^{L} f_i a_{r-i} = 0$, то для любого $\delta \in F$ выполнено равенство $\sum\limits_{i=0}^{L} \widetilde{f}_i a_{r-i} = 0$, где $\widetilde{f}(x) = \delta \cdot f(x)$. Поэтому алгоритм 1 можно записать в следующем виде.

Алгоритм 1' (алгоритм Берлекэмпа — Месси).
Вход: последовательность $a_1, \ldots, a_n$ над некоторым полем.
Выход: LFSR $(L, f(x))$ минимальной длины L, для которого

$$-a_j = \sum_{i=1}^{L} f_i a_{j-i}, \quad j = L+1,\, L+2, \ldots, n.$$

1. Определить $r := 0$, $f(x) := 1$, $b(x) := 1$, $L := 0$, $\delta := 1$.
2. Цикл $r := 1, \ldots, n$:
   2.1. Определить $\Delta := \sum\limits_{i=0}^{L} f_i a_{r-i}$;
   2.2. Если $\Delta = 0$, то $b(x) := x \cdot b(x)$;
   2.3. Если $\Delta \neq 0$:
      2.3.1 $buf(x) := \delta \cdot f(x) - \Delta \cdot x \cdot b(x)$;
      2.3.2. Если $2L < r$:
         $b(x) := f(x)$,
         $f(x) := buf(x)$,
         $L := r - L$,
         $\delta := \Delta$;
      2.3.3. Иначе (т. е. выполнено $2L \geqslant r$):
         $f(x) := buf(x)$,
         $b(x) := x \cdot b(x)$;
3. $f(x) := f_0^{-1} \cdot f(x)$.

2. Взаимосвязь алгоритма Берлекэмпа — Месси и обобщенного алгоритма Евклида

Приведенный алгоритм Берлекэмпа — Месси при определенном ограничении можно заменить на эквивалентный алгоритм на основе обобщенного алгоритма Евклида. Этот факт отражен в нескольких работах, например в [5; 6]. В данной работе приведем другое доказательство данной эквивалентности.

Алгоритм 2 (нахождение решения системы (1) с помощью обобщенного алгоритма Евклида).
Вход: последовательность $a_1, a_2, \ldots, a_{2n}$ над некоторым полем F, для которой система (1) имеет решение.
Выход: многочлен $f(x)$ степени $\leqslant n$, для которого $f(0) = 1$ и

$$-a_j = \sum_{i=1}^{n} f_i a_{j-i}, \quad j = n+1,\, n+2, \ldots, 2n.$$

1. Определить $r_{-1}(x) = x^{2n},\ r_0(x) = \sum\limits_{i=1}^{2n} a_i x^{i-1},\ v_{-1}(x) = 0,\ v_0(x) = 1.$

2. Производится последовательность вычислений обобщенного алгоритма Евклида:

$$\begin{array}{l} r_{i-2}(x) = r_{i-1}(x)q_{i-1}(x) + r_i(x), \\ v_i(x) = v_{i-2}(x) - v_{i-1}(x)q_{i-1}(x), \\ i = 1, 2, \ldots, \end{array}$$

до тех пор, пока для некоторого $r_j(x)$ не будет выполнено условие

$$\deg r_{j-1}(x) \geqslant n, \quad \deg r_j(x) \leqslant n-1.$$

3. Определить $f(x) = \lambda v_j(x)$, где константа $\lambda \in F$ задается так, чтобы удовлетворялось условие $f(0) = 1$.

Теорема 2. Если для последовательности $a_1, a_2, \ldots, a_{2n}$ над некоторым полем F система (1) имеет решение, то алгоритм 2 всегда возвращает решение системы (1). Более того, если $f_1, \ldots, f_n$ — некоторое решение системы (1), $f(x) = 1 + f_1 x + \ldots + f_n x^n$ — соответствующий многочлен, $\widetilde{f}(x)$ — результат работы алгоритма 2, то $\widetilde{f}(x)$ делит $f(x)$, т. е. из всех решений системы (1) многочлен $\widetilde{f}(x)$ имеет минимальную степень.

Доказательство. Пусть $f_1, \ldots, f_n$ — некоторое решение системы (1). Определим $f_0 = 1$ и обозначим:

$$\begin{array}{l} g_0 = a_1 f_0, \\ g_1 = a_2 f_0 + a_1 f_1, \\ \ldots \\ g_{n-1} = a_n f_0 + a_{n-1} f_1 + \ldots + a_1 f_{n-1}. \end{array} \tag{3}$$

Тогда на основе системы (1) получаем такую систему:

$$\begin{pmatrix} a_1 & 0 & \ldots & 0 & 0 \\ a_2 & a_1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_n & a_{n-1} & \ldots & a_1 & 0 \\ a_{n+1} & a_n & \ldots & a_2 & a_1 \\ a_{n+2} & a_{n+1} & \ldots & a_3 & a_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{2n} & a_{2n-1} & \ldots & a_{n+1} & a_n \end{pmatrix} \begin{pmatrix} f_0 \\ f_1 \\ \ldots \\ f_n \end{pmatrix} = \begin{pmatrix} g_0 \\ g_1 \\ \ldots \\ g_{n-1} \\ 0 \\ 0 \\ \ldots \\ 0 \end{pmatrix}, \tag{4}$$

в которой система их последних n уравнений полностью совпадает с системой (1). Пусть

$$a(x) = \sum_{i=1}^{2n} a_i x^{i-1}, \quad f(x) = \sum_{i=0}^{n} f_i x^i, \quad g(x) = \sum_{i=0}^{n-1} g_i x^i.$$

Система (4) эквивалентна сравнению

$$a(x)f(x) \equiv g(x) \pmod{x^{2n}} \tag{5}$$

с условиями

$$f(0) = 1, \quad \deg f(x) \leqslant n, \quad \deg g(x) \leqslant n-1. \tag{6}$$

Действительно, пусть выполнено сравнение (5) с условиями (6). Так как выполнено неравенство $\deg g(x) \leqslant n-1$, то коэффициенты многочлена $a(x)f(x)$ при степенях $x^n, x^{n+1}, \ldots, x^{2n-1}$ равны нулю. Это значит, что должны выполняться последние n уравнений системы (4). При этом первые n уравнений системы (4) напрямую следуют из сравнения (5). Обратно, из системы (4) очевидным образом следует сравнение (5) с условиями (6).

Применим к многочленам $r_{-1}(x) = x^{2n},\ r_0(x) = a(x),\ u_{-1}(x) = 1,\ u_0(x) = 0,\ v_{-1}(x) = 0,\ v_0(x) = 1$ обобщенный алгоритм Евклида:

$$\begin{array}{l} r_{i-2}(x) = r_{i-1}(x)q_{i-1}(x) + r_i(x), \\ u_i(x) = u_{i-2}(x) - u_{i-1}(x)q_{i-1}(x), \\ v_i(x) = v_{i-2}(x) - v_{i-1}(x)q_{i-1}(x), \\ i = 1, 2, \ldots \end{array}$$

Тогда на каждом шаге алгоритма будем получать равенства

$$u_i(x)x^{2n} + v_i(x)a(x) = r_i(x),$$

из которых следуют сравнения $v_i(x)a(x) \equiv r_i(x) \pmod{x^{2n}}$. Так как

$$2n = \deg r_{-1}(x) > \deg r_0(x) > \deg r_1(x) > \ldots,$$

то для некоторого j будут выполнены неравенства

$$\deg r_{j-1}(x) \geqslant n, \quad \deg r_j(x) \leqslant n-1.$$

Поэтому индекс j определен однозначно. При этом

$$\deg v_j(x) = \deg x^{2n} - \deg r_{j-1}(x) \leqslant 2n - n = n.$$

Следовательно, мы получили сравнение $v_j(x)a(x) \equiv r_j(x) \pmod{x^{2n}}$, где $\deg r_j(x) \leqslant n-1$, $\deg v_j(x) \leqslant n$.

Покажем, что $v_j(0) \neq 0$. Для многочленов $v_j(x)$ и $r_j(x)$, а также для многочленов $f(x)$, $g(x)$ и некоторого многочлена $t(x)$ выполнены равенства

$$u_j(x)x^{2n} + v_j(x)a(x) = r_j(x), \tag{7}$$

$$t(x)x^{2n} + f(x)a(x) = g(x). \tag{8}$$

Домножив обе части первого равенства на $f(x)$, а второго — на $v_j(x)$, получим

$$\begin{aligned} f(x)u_j(x)x^{2n} + f(x)v_j(x)a(x) = f(x)r_j(x), \\ v_j(x)t(x)x^{2n} + v_j(x)f(x)a(x) = v_j(x)g(x). \end{aligned} \tag{9}$$

Из данных равенств следует сравнение

$$f(x)r_j(x) \equiv v_j(x)g(x) \pmod{x^{2n}}.$$

Учитывая степени многочленов в данном сравнении, получаем равенство

$$f(x)r_j(x) = v_j(x)g(x).$$

Поэтому из (9) с учетом последнего равенства следует такое равенство:

$$f(x)u_j(x) = v_j(x)t(x).$$

Из свойства взаимной простоты многочленов $u_j(x)$ и $v_j(x)$ следует, что $v_j(x) \mid f(x)$, поэтому для некоторого многочлена $\mu(x)$ выполнено $f(x) = \mu(x)v_j(x)$. Подставим это равенство в (8):

$$t(x)x^{2n} + \mu(x)v_j(x)a(x) = g(x).$$

Теперь домножим равенство (7) на $\mu(x)$:

$$\mu(x)u_j(x)x^{2n} + \mu(x)v_j(x)a(x) = \mu(x)r_j(x).$$

Учитывая степени многочленов $g(x)$, $\mu(x)$ и $r_j(x)$, из последних двух равенств следует равенство $g(x) = \mu(x)r_j(x)$.

Таким образом, $f(x) = \mu(x)v_j(x)$, $g(x) = \mu(x)r_j(x)$. Так как $f(0) = 1$, то выполнено $v_j(0) \neq 0$.

Определим $\widetilde{f}(x) = \lambda v_j(x)$, где константа $\lambda \in F$ задается так, чтобы удовлетворялось условие $\widetilde{f}(0) = 1$. Тогда из $\lambda v_j(x)a(x) \equiv \lambda r_j(x) \pmod{x^{2n}}$, $\deg \lambda v_j(x) \leqslant n$ получаем, что $\widetilde{f}_1, \ldots, \widetilde{f}_n$ — решение системы (1). При этом $\widetilde{f}(x) \mid f(x)$. □

Предложение 1. Пусть $(L, f(x))$ — результат работы алгоритма 1, которому на вход подавалась последовательность $a_1, \ldots, a_n$. Пусть

$$\begin{aligned} &g_0 = a_1 f_0, \\ &g_1 = a_2 f_0 + a_1 f_1, \\ &\ldots \\ &g_{L-1} = a_L f_0 + a_{L-1} f_1 + \ldots + a_1 f_{L-1}, \end{aligned} \tag{10}$$

где $f_0 = 1$. Тогда $L = \max\{\deg f(x), \deg g(x) + 1\}$, где $g(x) = g_0 + g_1 x + \ldots + g_{L-1}x^{L-1}$.

Доказательство. Очевидно, что $L \geqslant \max\{\deg f(x), \deg g(x) + 1\}$. Предположим, что $L > \max\{\deg f(x), \deg g(x) + 1\}$. В этом случае $f_L = 0 = g_{L-1}$. Из равенств (2) и $f_L = 0$ следуют равенства

$$a_j = -\sum_{i=1}^{L-1} f_i a_{j-i}, \quad j = L+1, L+2, \ldots, n.$$

Из равенства $g_{L-1} = 0$, учитывая (10), получаем такое равенство:

$$a_L + a_{L-1} f_1 + \ldots + a_1 f_{L-1} = 0.$$

Поэтому будут выполнены такие равенства:

$$a_j = -\sum_{i=1}^{L-1} f_i a_{j-i}, \quad j = L, L+1, \ldots, n.$$

Это значит, что алгоритм 1 возвратил LFSR $(L, f(x))$ не минимальной длины, что противоречит тому, что алгоритм Берлекэмпа — Месси возвращает LFSR минимальной длины. □

Следующая теорема показывает, что в случае совместности системы (1) алгоритмы 1 и 2 эквивалентны.

Теорема 3. Пусть для последовательности $a_1, a_2, \ldots, a_{2n}$ над некоторым полем F система (1) имеет решение. Пусть $(L, f(x))$ — результат работы алгоритма 1, которому на вход подается данная последовательность, $\widetilde{f}(x)$ — результат работы алгоритма 2. Тогда $f(x) = \widetilde{f}(x)$.

Доказательство. Пусть $(L, f(x))$ — результат работы алгоритма 1, $g(x)$ — многочлен, вычисленный с помощью формул (10), $\widetilde{f}(x) = \lambda v_j(x)$, $\widetilde{g}(x) = \lambda r_j(x)$ — результат работы алгоритма 2. По предложению 1 выполнено равенство $L = \max\{\deg f(x), \deg g(x) + 1\}$. По теореме 2 для некоторого многочлена $\mu(x) \in F[x]$ выполнены равенства $f(x) = \mu(x)\widetilde{f}(x)$, $g(x) = \mu(x)\widetilde{g}(x)$. Обозначим $\widetilde{L} = \max\{\deg \widetilde{f}(x), \deg \widetilde{g}(x) + 1\}$. Тогда

$$-a_j = \sum_{i=1}^{\widetilde{L}} \widetilde{f}_i a_{j-i}, \quad j = \widetilde{L}+1, \widetilde{L}+2, \ldots, 2n.$$

Предположим, что $\deg \mu(x) \geqslant 1$. Тогда из неравенств $\deg f(x) > \deg \widetilde{f}(x)$, $\deg g(x) > \deg \widetilde{g}(x)$ следует, что $\widetilde{L} < L$, т. е. LFSR $(L, f(x))$ имеет не минимальную длину. Противоречие со свойством минимальности длины LFSR алгоритма Берлекэмпа — Месси.

Таким образом, $\mu(x)$ является многочленом нулевой степени. Так как $f(0) = 1 = \widetilde{f}(0)$, то $\mu(x) = 1$. □

Следствие 1. Алгоритм 2 возвращает LFSR $(L, f(x))$ минимальной длины $L = \max\{\deg v_j(x), \deg r_j(x) + 1\}$.

3. Алгоритм Берлекэмпа — Месси в случае поля характеристики два

Хорошо известно следующее утверждение (см., напр., [1]).

Теорема 4. Пусть F — поле характеристики два, $a_1, a_2, \ldots, a_{2n} \in F$, $a_{2i} = a_i^2$ для любого $i = 1, \ldots, n-1$. Пусть $(L, f(x))$ — LFSR, построенный для последовательности $a_1, a_2, \ldots, a_{2n-1}$, причем $L \leqslant n-1$. Тогда следующие условия эквивалентны:

1) $a_{2n} = \sum\limits_{i=1}^{L} f_i a_{2n-i}$, т. е. элемент a_{2n} можно получить с помощью LFSR $(L, f(x))$;
2) $a_{2n} = a_n^2$.

Следствие 2. Пусть F — поле характеристики два, $a_1, a_2, \ldots, a_{2n} \in F$, для которой система (1) имеет решение, причем $a_{2i} = a_i^2$ для любого $i = 1, \ldots, n$. Если к данной последовательности применить алгоритм Берлекэмпа — Месси, то $\Delta_{2i} = 0$ для любого $i = 1, \ldots, n$.

Следствие 2 показывает, что для указанной последовательности $a_1, a_2, \ldots, a_{2n}$ в алгоритме Берлекэмпа — Месси достаточно рассматривать только итерации с нечетными номерами, что ускоряет алгоритм 1. Этот момент отражен в следующем алгоритме.

Алгоритм 3 (алгоритм Берлекэмпа — Месси для случая $\operatorname{char} F = 2$).

Вход: последовательность $a_1, a_2, \ldots, a_{2n} \in F$, $\operatorname{char} F = 2$, для которой система (1) имеет решение, причем $a_{2i} = a_i^2$ для любого $i = 1, \ldots, n$.

Выход: LFSR $(L, f(x))$ минимальной длины L, для которого

$$a_j = \sum_{i=1}^{L} f_i a_{j-i}, \quad j = L+1,\ L+2, \ldots, 2n. \tag{11}$$

1. Определить $r := 0,\ f(x) := 1,\ b(x) := 1,\ L := 0.$
2. Если $a_1 = 0$, то $b(x) := x$.
3. Иначе (т. е. если $a_1 \neq 0$) :
   $f(x) := 1 + a_1 \cdot x, \quad b(x) := a_1^{-1}, \quad L := 1.$
4. Цикл $i := 2, \ldots, n$:
   4.1. Определить $r := 2i - 1$;
   4.2. Определить $\Delta := a_r + \sum\limits_{i=1}^{L} f_i a_{r-i}$;
   4.3. Если $\Delta = 0$, то $b(x) := x^2 \cdot b(x)$;
   4.4. Если $\Delta \neq 0$:
      4.4.1. Если $2L < r$:
         $buf(x) := f(x) + \Delta \cdot x^2 \cdot b(x)$,
         $b(x) := \Delta^{-1} \cdot f(x)$,
         $f(x) := buf(x)$,
         $L := r - L$;
      4.4.2. Иначе (т. е. выполнено $2L \geqslant r$):
         $f(x) := f(x) + \Delta \cdot x^2 \cdot b(x)$,
         $b(x) := x^2 \cdot b(x)$.

4. Декодирование кодов БЧХ и кодов Рида — Соломона с использованием алгоритма Берлекэмпа — Месси

Кодом Боуза — Чоудхури — Хоквингема (БЧХ) над полем $GF(q)$ называется такой циклический код длины n, порождающий многочлен $g(x)$ наименьшей степени которого имеет своими корнями последовательность идущих подряд степеней некоторого произвольного элемента $\alpha \in GF(q^m)$: $: \alpha^b,\ \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$, где b — некоторое неотрицательное целое число, $\delta \geqslant 2$, причем

$$n = \begin{cases} \mathrm{ord}(\alpha), & \delta > 2, \\ \mathrm{ord}(\alpha^b), & \delta = 2, \end{cases}$$

где ord — порядок элемента. Из данного определения следует, что длина кода n делит число $q^m - 1$ (порядок мультипликативной группы поля $GF(q^m)$).

Кодом Рида — Соломона (РС) называется код БЧХ над полем $GF(q)$, $q > 2$, который имеет длину $q-1$. Из данного определения следует, что при $\delta > 2$ выполнены такие условия: $\alpha \in GF(q)$ и α является примитивным элементом поля $GF(q)$. Также из этого определения следует, что порождающий многочлен кода РС имеет вид

$$g(x) = (x - \alpha^b)(x - \alpha^{b+1}) \ldots (x - \alpha^{b+\delta-2}),$$

т. е. коэффициенты данного многочлена принадлежат полю $GF(q)$. Хорошо известно, что коды РС являются МДР-кодами, т. е. кодами с максимально достижимым расстоянием ($d = n - k + 1$).

Рассмотрим случай, когда в канале связи действуют ошибки и стирания. Заметим, что в полученных ниже алгоритмах достаточно положить $s = 0$ (число стираний), чтобы рассматривать случай только ошибок.

Пусть A — $[n, k, d-n-k+1]$-код РС над полем $GF(q)$, d — кодовое расстояние, $u \in A$ — переданный вектор. Пусть v — полученный на приемной стороне вектор (после отправки u), в котором могут быть ошибки и стирания. Пусть t — максимальное число возможных ошибок при фиксированном числе стираний s в векторе v, $d \geqslant 2t + s + 1$, $t = [(d - s - 1)/2]$, m — реальное число ошибок, $m \leqslant t$. Так как позиции стертых символов известны, то при $s > 0$ заменим эти символы в векторе v на нули и будем обращаться с полученным вектором $\widetilde{v}$ как с вектором, содержащим только ошибки. Пусть ошибки произошли на позициях $i_1, \ldots, i_m$, а стирания — на позициях $i_{m+1}, \ldots, i_{m+s}$. При этом известны только позиции $i_{m+1}, \ldots, i_{m+s}$. После того как на данные позиции поместили нули, с какими-то позициями могли угадать (если в кодовом векторе там действительно стояли нули). Поэтому $\widetilde{v} = u + e$, где e — вектор ошибок веса не более $m + s$.

Пусть $X_1 = \alpha^{i_1}, \ldots, X_m = \alpha^{i_m}$ — неизвестные локаторы ошибок, $X_{m+1} = \alpha^{i_{m+1}}, \ldots, X_{m+s} = \alpha^{i_{m+s}}$ — известные локаторы стираний, $Y_1 = e_{i_1}, \ldots, Y_{m+s} = e_{i_{m+s}}$ — значения ошибок в векторе $\widetilde{v}$. Найдем компоненты синдромного вектора:

$$\begin{aligned}
&S_0 = \widetilde{v}(\alpha) = Y_1 X_1 + \ldots + Y_m X_m + Y_{m+1} X_{m+1} + \ldots + Y_{m+s} X_{m+s}, \\
&S_1 = \widetilde{v}(\alpha^2) = Y_1 X_1^2 + \ldots + Y_m X_m^2 + Y_{m+1} X_{m+1}^2 + \ldots + Y_{m+s} X_{m+s}^2, \\
&\ldots \\
&S_{2t+s-1} = \widetilde{v}(\alpha^{2t+s}) = Y_1 X_1^{2t+s} + \ldots + Y_m X_m^{2t+s} + Y_{m+1} X_{m+1}^{2t+s} + \ldots + Y_{m+s} X_{m+s}^{2t+s}.
\end{aligned}$$

Запишем синдромный многочлен в виде

$$S(x)=\sum_{i=0}^{2t+s-1}S_ix^i=\sum_{i=0}^{2t+s-1}\left(\sum_{j=1}^{m+s}Y_jX_j^{i+1}\right)x^i=\sum_{j=1}^{m+s}Y_jX_j\left(\sum_{i=0}^{2t+s-1}(X_jx)^i\right)=$$

$$=\sum_{j=1}^{m+s}Y_jX_j\frac{1-(X_jx)^{2t+s}}{1-X_jx}=\sum_{j=1}^{m+s}\frac{Y_jX_j}{1-X_jx}-x^{2t+s}\sum_{j=1}^{m+s}\frac{Y_jX_j^{2t+s+1}}{1-X_jx}.$$

Полагая

$$\widetilde{\sigma}(x)=\prod_{i=1}^{m+s}(1-X_ix)=\sum_{i=0}^{m+s}\widetilde{\sigma}_ix^i,\quad \widetilde{\sigma}_0=1,$$

$$\widetilde{\omega}(x)=\sum_{i=1}^{m+s}Y_iX_i\prod_{\substack{1\leqslant j\leqslant m+s,\\ j\neq i}}(1-X_jx),\quad \widetilde{\Phi}(x)=\sum_{i=1}^{m+s}Y_iX_i^{2t+s+1}\prod_{\substack{1\leqslant j\leqslant m+s,\\ j\neq i}}(1-X_jx),$$

после приведения всех дробей к общему знаменателю получим

$$S(x)=\frac{\widetilde{\omega}(x)}{\widetilde{\sigma}(x)}-x^{2t+s}\frac{\widetilde{\Phi}(x)}{\widetilde{\sigma}(x)}.$$

Тогда

$$S(x)\widetilde{\sigma}(x)=\widetilde{\omega}(x)-x^{2t+s}\widetilde{\Phi}(x).$$

Данное выражение называют ключевым уравнением, которому можно придать иной вид:

$$\widetilde{\sigma}(x)S(x)\equiv\widetilde{\omega}(x)\pmod{x^{2t+s}}. \tag{12}$$

Заметим, что $\widetilde{\sigma}(x)=\sigma(x)\nu(x)$, где $\sigma(x)$ — это многочлен неизвестных локаторов ошибок, $\nu(x)$ — многочлен известных локаторов стираний:

$$\widetilde{\sigma}(x)=\prod_{i=1}^{m}(1-X_ix)\prod_{i=1}^{s}(1-X_{m+i}x)=\sigma(x)\nu(x).$$

Введем в рассмотрение многочлен $\widetilde{S}(x)=S(x)\nu(x)$ — модифицированный синдромный многочлен. Тогда ключевое уравнение (12) примет вид

$$\sigma(x)\widetilde{S}(x)\equiv\widetilde{\omega}(x)\pmod{x^{2t+s}}, \tag{13}$$

где

$$\deg\sigma(x)\leqslant m,\quad \deg\widetilde{\omega}(x)\leqslant m+s-1,\quad \sigma(0)=1. \tag{14}$$

Пусть

$$\widetilde{S}(x)=\widetilde{S}_0+\widetilde{S}_1x+\ldots+\widetilde{S}_{2t+2s-1}x^{2t+2s-1}=$$

$$=S(x)\nu(x)=(S_0+S_1x+\ldots+S_{2t+s-1}x^{2t+s-1})(\nu_0+\nu_1x+\ldots+\nu_sx^s),$$

где $\nu_0=1$, $\nu_i=(-1)^i\sigma_i(X_{m+1},\ldots,X_{m+s})$ — элементарный симметрический многочлен от $X_{m+1},\ldots,X_{m+s}$, $i=1,\ldots,s$.

Так как в сравнении (13) $\deg\widetilde{\omega}(x)\leqslant m+s-1$, $\deg\widetilde{S}(x)\leqslant 2t+2s-1$, $\deg\sigma(x)\leqslant m$, то необходимым условием выполнения данного сравнения является тот факт, что коэффициенты многочлена $\sigma(x)\widetilde{S}(x)$ при степенях $j=m+s,m+s+1,\ldots,2t+s-1$ равны нулю. Поэтому получаем такую систему линейных уравнений:

$$\begin{cases}\sigma_0\widetilde{S}_{s+m}+\sigma_1\widetilde{S}_{s+m-1}+\ldots+\sigma_m\widetilde{S}_s=0,\\ \sigma_0\widetilde{S}_{s+m+1}+\sigma_1\widetilde{S}_{s+m}+\ldots+\sigma_m\widetilde{S}_{s+1}=0,\\ \ldots\\ \sigma_0\widetilde{S}_{s+2t-1}+\sigma_1\widetilde{S}_{s+2t-2}+\ldots+\sigma_m\widetilde{S}_{s+2t-m-1}=0.\end{cases}$$

Так как $\sigma_0=1$, то данная система в матричной форме примет такой вид:

$$\begin{pmatrix}\widetilde{S}_{s+m-1} & \widetilde{S}_{s+m-2} & \ldots & \widetilde{S}_s\\ \widetilde{S}_{s+m} & \widetilde{S}_{s+m-1} & \ldots & \widetilde{S}_{s+1}\\ \ldots & \ldots & \ldots & \ldots\\ \widetilde{S}_{s+2t-2} & \widetilde{S}_{s+2t-3} & \ldots & \widetilde{S}_{s+2t-m-1}\end{pmatrix}\begin{pmatrix}\sigma_1\\ \sigma_2\\ \ldots\\ \sigma_m\end{pmatrix}=\begin{pmatrix}-\widetilde{S}_{s+m}\\ -\widetilde{S}_{s+m+1}\\ \ldots\\ -\widetilde{S}_{s+2t-1}\end{pmatrix}. \tag{15}$$

Будем искать решение данной системы с помощью алгоритма Берлекэмпа — Месси.

Теорема 5. Пусть $d \geqslant 2t+s+1$, $m \leqslant t$. Если на вход алгоритма 1 подать последовательность $\widetilde{S}_s$, $\widetilde{S}_{s+1}, \ldots, \widetilde{S}_{s+2t-1}$, то на выходе алгоритма будет верное значение многочлена локаторов ошибок $\sigma(x)$.

Доказательство. Пусть $\widetilde{\sigma}(x)$ — многочлен, полученный после применения алгоритма 1. Так как коэффициенты многочлена локаторов ошибок $\sigma(x)$ являются решением системы (15), то в теореме 1 будет выполнено неравенство $L \leqslant m$. Удалив в системе (15) $2t-2m$ последних уравнений, получим новую систему с квадратной матрицей системы порядка m. Из теоремы 5 работы [7] следует, что данная матрица невырождена, поэтому полученная новая система имеет единственное решение. Это значит, что $\widetilde{\sigma}(x) = \sigma(x)$ и $L = m$. □

Учитывая теорему 5, получаем следующий алгоритм декодирования кодов РС (кодов БЧХ).

Алгоритм 4 (декодирование кода РС на основе алгоритма Берлекэмпа — Месси на случай ошибок и стираний).

Вход: принятый вектор v, в котором s стираний и не более t ошибок.

Выход: исходный кодовый вектор u, если $d \geqslant 2t+s+1$.

1. Определяется $t = [(d-s-1)/2]$. В векторе v все стирания заменяют нулями, получая тем самым вектор $\widetilde{v}$. Находятся компоненты $S_0, S_1, \ldots, S_{2t+s-1}$ синдромного вектора: $S_i = \widetilde{v}(\alpha^{i+1})$, $i = 0, 1, \ldots, 2t+s-1$. Если они все равны нулю, то возвращается вектор $\widetilde{v}$ и процедура окончена.

   Вычисляются значения локаторов стираний $X_{t+1} = \alpha^{i_{t+1}}, \ldots, X_{t+s} = \alpha^{i_{t+s}}$ на основе известных позиций стираний $i_{t+1}, \ldots, i_{t+s}$. Вычисляются коэффициенты модифицированного синдромного многочлена $\widetilde{S}(x)$ (если $s=0$, то $\widetilde{S}(x) = S(x)$).

2. На вход алгоритма 1 подается последовательность $\widetilde{S}_s$, $\widetilde{S}_{s+1}, \ldots, \widetilde{S}_{s+2t-1}$. На выходе данного алгоритма получается многочлен $\sigma(x)$. Пусть $l = \deg \sigma(x)$.

3. Отыскиваются l корней многочлена $\sigma(x)$ последовательной подстановкой в него ненулевых элементов поля F. При этом локаторы ошибок — это величины, обратные корням многочлена $\sigma(x)$.

4. Определяется множество $M = \{1, \ldots, l\} \cup \{t+1, \ldots, t+s\}$. По формулам Форни

$$Y_j = \frac{X_j^{-1}\widetilde{\omega}(X_j^{-1})}{\prod\limits_{i \in M \setminus \{j\}} (1 - X_i X_j^{-1})}, \quad j \in M, \tag{16}$$

где $\widetilde{\omega}(x) \equiv \sigma(x)\widetilde{S}(x) \pmod{x^{2t+s}}$, находятся значения ошибок Y_j, $j \in M$. У вектора $\widetilde{v}$ из i_j-го символа, $X_j = \alpha^{i_j}$, вычитается значение Y_j, $j \in M$. При этом получается кодовый вектор u.

Пример 1. Рассмотрим расширение поля $GF(2) \subset GF(2^4)$. Пусть поле $GF(2^4)$ строится на основе примитивного многочлена $p(x) = x^4 + x + 1$, α — примитивный элемент поля $GF(2^4)$:

$$\begin{array}{rcccccl}
\alpha^0 = & 1 & & & = & 1000, & \alpha^1 = \quad \alpha \quad = 0100, \\
\alpha^2 = & & & \alpha^2 & = & 0010, & \alpha^3 = \quad \alpha^3 = 0001, \\
\alpha^4 = & 1 & +\alpha & & = & 1100, & \alpha^5 = \quad \alpha \quad +\alpha^2 = 0110, \\
\alpha^6 = & & & \alpha^2 & +\alpha^3 = & 0011, & \alpha^7 = 1 \quad +\alpha \quad +\alpha^3 = 1101, \\
\alpha^8 = & 1 & & +\alpha^2 & = & 1010, & \alpha^9 = \quad \alpha \quad +\alpha^3 = 0101, \\
\alpha^{10} = & 1 & +\alpha & +\alpha^2 & = & 1110, & \alpha^{11} = \quad \alpha \quad +\alpha^2 \quad +\alpha^3 = 0111, \\
\alpha^{12} = & 1 & +\alpha & +\alpha^2 & +\alpha^3 = & 1111, & \alpha^{13} = 1 \quad +\alpha^2 \quad +\alpha^3 = 1011, \\
\alpha^{14} = & 1 & & & +\alpha^3 = & 1001, & \alpha^{15} = 1 \quad = 1000.
\end{array}$$

Рассмотрим код Рида — Соломона с параметрами $n = 15$, $k = 7$, $d = 9$. В этом случае код может исправить четыре и менее ошибок, либо три и менее ошибок и два и менее стираний, либо две и менее ошибок и четыре и менее стираний, либо одну ошибку и шесть и менее стираний, либо восемь и менее стираний.

Рассмотрим случай возможности исправления до двух ошибок и до четырех стираний. Пусть на приемном конце получен вектор

$$v = \left(\alpha^7, \quad \alpha^{10}, \quad \alpha, \quad 1, \quad \alpha^{12}, \quad \alpha^{12}, \quad \alpha^5, \quad *, \quad \alpha^2, \quad *, \quad *, \quad \alpha^6, \quad *, \quad \alpha^3, \quad 1 \right),$$

в котором не более двух ошибок и четыре стирания. Применим алгоритм декодирования 4.

1. Полагаем $s = 4$, $t = [(d-s-1)/2] = 2$. В данном случае нам известно, что

$$X_3 = \alpha^7, X_4 = \alpha^9, X_5 = \alpha^{10}, X_6 = \alpha^{12}.$$

Поэтому

$$\nu(x) = (1-\alpha^7 x)(1-\alpha^9 x)(1-\alpha^{10}x)(1-\alpha^{12}x) = \\ = 1+\alpha^{14}x+x^2+\alpha^3x^3+\alpha^8x^4.$$

Заменим в векторе v $*$ на 0:

$$\widetilde{v} = \left(\ \alpha^7,\ \ \alpha^{10},\ \ \alpha,\ \ 1,\ \ \alpha^{12},\ \ \alpha^{12},\ \ \alpha^5,\ \ 0,\ \ \alpha^2,\ \ 0,\ \ 0,\ \ \alpha^6,\ \ 0,\ \ \alpha^3,\ \ 1\ \right).$$

Вычислим компоненты синдрома для вектора $\widetilde{v}$:

$$S_0 = \widetilde{v}(\alpha) = \alpha^8,\ \ S_1 = \widetilde{v}(\alpha^2) = \alpha^5,\ \ S_2 = \widetilde{v}(\alpha^3) = \alpha^4,$$
$$S_3 = \widetilde{v}(\alpha^4) = \alpha^7,\ \ S_4 = \widetilde{v}(\alpha^5) = \alpha^4,\ \ S_5 = \widetilde{v}(\alpha^6) = \alpha^{11},$$
$$S_6 = \widetilde{v}(\alpha^7) = \alpha^7,\ \ S_7 = \widetilde{v}(\alpha^8) = \alpha^9.$$

Поэтому синдромный многочлен имеет такой вид:

$$S(x) = \alpha^8+\alpha^5x+\alpha^4x^2+\alpha^7x^3+\alpha^4x^4+\alpha^{11}x^5+\alpha^7x^6+\alpha^9x^7.$$

Тогда

$$\widetilde{S}(x) = S(x)\nu(x) = \widetilde{S}_0+\widetilde{S}_1x+\ldots+\widetilde{S}_{11}x^{11} = \\ = \alpha^8+\alpha^{13}x+\alpha^8x^2+\alpha^7x^3+\alpha^7x^4+\alpha^7x^5+\alpha^{10}x^6+\alpha x^7+\alpha^3x^8+\alpha^{11}x^9+\alpha^{11}x^{10}+\alpha^2x^{11}.$$

2. На вход алгоритма 1 подаем последовательность $\widetilde{S}_4 = \alpha^7$, $\widetilde{S}_5 = \alpha^7$, $\widetilde{S}_6 = \alpha^{10}$, $\widetilde{S}_7 = \alpha$. После вычислений

r	Δ	$\sigma(x)$	$b(x)$	L
0		1	1	0
1	α^7	$1+\alpha^7x$	α^8	1
2	α	$1+x$	α^8x	1
3	α^6	$1+x+\alpha^{14}x^2$	$\alpha^9+\alpha^9x$	2
4	α^{14}	$1+\alpha^2x+\alpha^6x^2$	$\alpha^9x+\alpha^9x^2$	2

получаем $\sigma(x) = 1+\alpha^2x+\alpha^6x^2$.

3. Корнями многочлена локаторов ошибок $\sigma(x)$ являются $x_1 = \alpha^{14}$, $x_2 = \alpha^{10}$, поэтому $X_1 = \alpha$, $X_2 = \alpha^5$.

4. После того как все локаторы ошибок известны, можно воспользоваться формулой Форни для кодов РС

$$Y_i = \frac{X_i^{-1}\widetilde{\omega}(X_i^{-1})}{\prod\limits_{\substack{1\leqslant j\leqslant t+s,\\ j\neq i}}(1-X_jX_i^{-1})},\quad i = 1,2,\ldots,t+s,$$

где

$$\widetilde{\omega}(x) \equiv \sigma(x)\widetilde{S}(x) \equiv \\ \equiv \alpha^8+\alpha^9x+\alpha^{13}x^2+\alpha^{12}x^3+\alpha^3x^4+\alpha^6x^5 \pmod{x^8}.$$

Находим значения ошибок: $Y_1 = \alpha^6, Y_2 = \alpha, Y_3 = 0,\ Y_4 = \alpha^6, Y_5 = \alpha^{10},\ Y_6 = \alpha^{11}$. Таким образом:

$$e = \left(\ 0,\ \ \alpha^6,\ \ 0,\ \ 0,\ \ 0,\ \ \alpha,\ \ 0,\ \ 0,\ \ 0,\ \ \alpha^6,\ \ \alpha^{10},\ \ 0,\ \ \alpha^{11},\ \ 0,\ \ 0\ \right),$$
$$u = v-e = \left(\ \alpha^7,\ \ \alpha^7,\ \ \alpha,\ \ 1,\ \ \alpha^{12},\ \ \alpha^{13},\ \ \alpha^5,\ \ 0,\ \ \alpha^2,\ \ \alpha^6,\ \ \alpha^{10},\ \ \alpha^6,\ \ \alpha^{11},\ \ \alpha^3,\ \ 1\ \right).$$

5. Декодирование двоичных кодов БЧХ с использованием алгоритма Берлекэмпа — Месси

В данном параграфе рассмотрим случай только ошибок для возможности применения алгоритма 3. На основе алгоритмов 3 и 4 получаем следующий алгоритм декодирования.

Алгоритм 5 (декодирование двоичного кода БЧХ на основе алгоритма Берлекэмпа — Месси).
Вход: полученный вектор v.
Выход: исходный кодовый вектор u, если произошло не более $[(d-1)/2]$ ошибок.

1. Определяется $t = [(d-1)/2]$. Находятся компоненты $S_0, S_1, \ldots, S_{2t-1}$ синдромного вектора: $S_i = v(\alpha^{i+1})$, $i = 0,1,\ldots,2t-1$. Если синдромный вектор нулевой, то алгоритм завершается и возвращается $u = v$.

2. Для последовательности $S_0, S_1, \ldots, S_{2t-1}$ с помощью алгоритма 3 находится многочлен локаторов ошибок $\sigma(x)$. Пусть $l = \deg\sigma(x)$.

3. Отыскиваются l корней многочлена $\sigma(x)$. При этом локаторы ошибок — это величины, обратные корням многочлена $\sigma(x)$.

   У вектора v из символа с номером i_j, $X_j = \alpha^{i_j}$, вычитается 1, $j = 1, \ldots, l$. Тем самым получается вектор u.

Пример 2. Пусть поле $GF(2^4)$ порождается примитивным многочленом $p(x) = x^4 + x + 1$ (см. пример 1), код БЧХ длины $n = 15$ порождается многочленом:

$$g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}.$$

В данном случае $k = 15 - 10 = 5$. Подряд идущиц корнями многочлена $g(x)$ будут:

$$\alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4,\ \alpha^5,\ \alpha^6.$$

Поэтому конструктивное расстояние данного кода равно $d = 7$, т. е. код гарантированно может исправлять до трех ошибок.

Пусть на приемном конце получен вектор

$$v = \begin{pmatrix} 1, & 1, & 0, & 0, & 1, & 0, & 0, & 1, & 1, & 0, & 1, & 0, & 1, & 1, & 0 \end{pmatrix},$$

в котором не более трех ошибок. Данный вектор соответствует многочлену

$$v(x) = 1 + x + x^4 + x^7 + x^8 + x^{10} + x^{12} + x^{13}.$$

Вычисляем

$$\begin{aligned}
&S_0 = v(\alpha) = 1 + \alpha + \alpha^4 + \alpha^7 + \alpha^8 + \alpha^{10} + \alpha^{12} + \alpha^{13} = \alpha^7,\\
&S_2 = v(\alpha^3) = 1 + \alpha^3 + \alpha^{12} + \alpha^6 + \alpha^9 + 1 + \alpha^6 + \alpha^9 = \alpha^{10},\\
&S_4 = v(\alpha^5) = 1 + \alpha^5 + \alpha^5 + \alpha^5 + \alpha^{10} + \alpha^5 + 1 + \alpha^5 = 1,\\
&S_1 = S_0^2 = \alpha^{14}, \quad S_3 = S_1^2 = \alpha^{13}, \quad S_5 = S_2^2 = \alpha^5.
\end{aligned}$$

Применим к этой последовательности алгоритм 3

r	Δ	$\sigma(x)$	$b(x)$	L
0		1	1	0
1	α^7	$1 + \alpha^7 x$	α^8	1
3	α^7	$1 + \alpha^7 x + x^2$	$\alpha^8 + x$	2
5	0	$1 + \alpha^7 x + x^2$	$\alpha^8 x^2 + x^3$	2

Поэтому многочлен локаторов ошибок имеет вид

$$\sigma(x) = 1 + \alpha^7 x + x^2.$$

Находим корни многочлена $\sigma(x)$: $x_1 = \alpha^{14}$, $x_2 = \alpha$. Поэтому

$$X_1 = x_1^{-1} = \alpha,\ \ X_2 = x_2^{-1} = \alpha^{14},$$

$$e = \begin{pmatrix} 0, & 1, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 1 \end{pmatrix},$$

$$u = v - e = \begin{pmatrix} 1, & 0, & 0, & 0, & 1, & 0, & 0, & 1, & 1, & 0, & 1, & 0, & 1, & 1, & 1 \end{pmatrix}.$$

6. Декодирование обобщенных кодов Рида — Соломона с использованием алгоритма Берлекэмпа — Месси

Рассматриваемая в данном параграфе теория частично отражена в работе [8], являющейся продолжением работы [7]. Эти две работы посвящены описанию различных алгоритмов декодирования обобщенных кодов Рида — Соломона на случай ошибок и стираний. Так как данная работа посвящена алгоритмам декодирования на основе алгоритма Берлекэмпа — Месси, то для удобства читателя приведем алгоритм декодирования и здесь.

Пусть $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$, где α_i — различные элементы поля $F = GF(q)$, $y = (y_0, y_1, \ldots, y_{n-1})$ — ненулевые (не обязательно различные) элементы из F. Тогда обобщенный код Рида — Соломона (ОРС), обозначаемый $GRS_k(\alpha, y)$, состоит из всех кодовых векторов вида

$$u = (y_0 b(\alpha_0), y_1 b(\alpha_1), \ldots, y_{n-1} b(\alpha_{n-1})), \tag{17}$$

где $b(x)$ — информационные многочлены над полем F степени не выше $k-1$. Кодовое расстояние кода $GRS_k(\alpha, y)$ равно $d = n - k + 1$. Если $n = q - 1$, вектор y состоит из единиц и $\alpha_i = \alpha^i$, $i = 0, 1, \ldots, n-1$, где α — примитивный элемент поля F, то в этом случае получаем код Рида — Соломона.

Заметим, что, в отличие от кодов РС, в обобщенных кодах РС одна из компонент вектора α может быть нулевой, что нужно учитывать в алгоритмах декодирования.

Пусть v — полученный на приемной стороне вектор, в котором могут быть ошибки и стирания. Пусть t — максимальное число возможных ошибок при фиксированном числе стираний s в векторе v, $d \geqslant 2t+s+1$, $t=[(d-s-1)/2]$, m — реальное число ошибок, $m \leqslant t$. Как и ранее, заменим стертые символы в векторе v, например, на нули и будем обращаться с полученным вектором $\widetilde{v}$ как с вектором, содержащим только ошибки. Пусть ошибки произошли на позициях $i_1,\ldots,i_m$, а стирания — на позициях $i_{m+1},\ldots,i_{m+s}$. При этом известны только позиции $i_{m+1},\ldots,i_{m+s}$. Получаем $\widetilde{v}=u+e$, где e — вектор ошибок веса не более $m+s$.

Вычисляя синдромный вектор, получаем

$$S=\widetilde{v}H^T=eH^T=\left(\ \ldots,\quad e_{i_1},\quad \ldots,\quad e_{i_{m+s}},\quad \ldots\ \right)\times$$

$$\times\left(\begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_0 & \alpha_1 & \ldots & \alpha_{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_0^{n-k-1} & \alpha_1^{n-k-1} & \ldots & \alpha_{n-1}^{n-k-1} \end{pmatrix}\begin{pmatrix} w_0 & 0 & \ldots & 0 \\ 0 & w_1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & w_{n-1} \end{pmatrix}\right)^T,$$

$$S_j=Z_1X_1^j+\ldots+Z_mX_m^j+Z_{m+1}X_{m+1}^j+\ldots+Z_{m+s}Z_{m+s}^j,$$
$$j=0,1,\ldots,2t+s-1,$$

где $X_1=\alpha_{i_1},\ldots,$ $X_m=\alpha_{i_m}$ — неизвестные локаторы ошибок, $X_{m+1}=\alpha_{i_{m+1}},\ldots,$ $X_{m+s}=\alpha_{i_{m+s}}$ — известные локаторы стираний, $Y_1=e_{i_1},\ldots,Y_{m+s}=e_{i_{m+s}}$ — значения ошибок в векторе $\widetilde{v}$, $Z_j=Y_jw_{i_j}$, $j=1,\ldots,m+s$. Пусть $\sigma(x)$ — это многочлен неизвестных локаторов ошибок, $\nu(x)$ — многочлен известных локаторов стираний. Полагая

$$S(x)=\sum_{i=0}^{2t+s-1}S_ix^i,\quad \widetilde{S}(x)=S(x)\nu(x),\quad \widetilde{\sigma}(x)=\prod_{i=1}^{m}(1-X_ix)\prod_{i=1}^{s}(1-X_{m+i}x)=\sigma(x)\nu(x),$$

$$\widetilde{\omega}(x)=\sum_{i=1}^{m+s}Z_i\prod_{\substack{1\leqslant j\leqslant m+s,\\ j\neq i}}(1-X_jx),\quad \widetilde{\Phi}(x)=\sum_{i=1}^{m+s}Z_iX_i^{2t+s}\prod_{\substack{1\leqslant j\leqslant m+s,\\ j\neq i}}(1-X_jx),$$

получим ключевое уравнение

$$\sigma(x)\widetilde{S}(x)\equiv\widetilde{\omega}(x)\pmod{x^{2t+s}},\tag{18}$$

где

$$\deg\sigma(x)\leqslant m,\quad \deg\widetilde{\omega}(x)\leqslant m+s-1,\quad \sigma(0)=1.\tag{19}$$

Пусть

$$\widetilde{S}(x)=\widetilde{S}_0+\widetilde{S}_1x+\ldots+\widetilde{S}_{2t+2s-1}x^{2t+2s-1}=$$
$$=S(x)\nu(x)=(S_0+S_1x+\ldots+S_{2t+s-1}x^{2t+s-1})(\nu_0+\nu_1x+\ldots+\nu_sx^s),$$

где $\nu_0=1$, $\nu_i=(-1)^i\sigma_i(X_{m+1},\ldots,X_{m+s})$ — элементарный симметрический многочлен от $X_{m+1},\ldots,X_{m+s}$, $i=1,\ldots,s$.

Так как в сравнении (18) $\deg\widetilde{\omega}(x)\leqslant m+s-1$, $\deg\widetilde{S}(x)\leqslant 2t+2s-1$, $\deg\sigma(x)\leqslant m$, то необходимым условием выполнения данного сравнения является тот факт, что коэффициенты многочлена $\sigma(x)\widetilde{S}(x)$ при степенях $j=m+s,m+s+1,\ldots,2t+s-1$ равны нулю. Поэтому получаем такую систему линейных уравнений:

$$\begin{cases} \sigma_0\widetilde{S}_{s+m}+\sigma_1\widetilde{S}_{s+m-1}+\ldots+\sigma_m\widetilde{S}_s=0, \\ \sigma_0\widetilde{S}_{s+m+1}+\sigma_1\widetilde{S}_{s+m}+\ldots+\sigma_m\widetilde{S}_{s+1}=0, \\ \ldots \\ \sigma_0\widetilde{S}_{s+2t-1}+\sigma_1\widetilde{S}_{s+2t-2}+\ldots+\sigma_m\widetilde{S}_{s+2t-m-1}=0. \end{cases}$$

Так как $\sigma_0=1$, то данная система в матричной форме примет такой вид:

$$\begin{pmatrix} \widetilde{S}_{s+m-1} & \widetilde{S}_{s+m-2} & \ldots & \widetilde{S}_s \\ \widetilde{S}_{s+m} & \widetilde{S}_{s+m-1} & \ldots & \widetilde{S}_{s+1} \\ \ldots & \ldots & \ldots & \ldots \\ \widetilde{S}_{s+2t-2} & \widetilde{S}_{s+2t-3} & \ldots & \widetilde{S}_{s+2t-m-1} \end{pmatrix}\begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \ldots \\ \sigma_m \end{pmatrix}=\begin{pmatrix} -\widetilde{S}_{s+m} \\ -\widetilde{S}_{s+m+1} \\ \ldots \\ -\widetilde{S}_{s+2t-1} \end{pmatrix}.\tag{20}$$

Теорема 6. Пусть $d\geqslant 2t+s+1$, $m\leqslant t$. Если на вход алгоритма 1 подать последовательность $\widetilde{S}_s$, $\widetilde{S}_{s+1},\ldots,$ $\widetilde{S}_{s+2t-1}$, то на выходе алгоритма будет верное значение многочлена локаторов ошибок $\sigma(x)$.

Доказательство аналогично доказательству теоремы 5. □

Алгоритм 6 (декодирование обобщенного кода РС на основе алгоритма Берлекэмпа — Месси на случай ошибок и стираний).

Вход: принятый вектор v, в котором s стираний и не более t ошибок.

Выход: исходный кодовый вектор u, если $d \geqslant 2t + s + 1$.

1. Определяется $t = [(d - s - 1)/2]$. В векторе v все стирания заменяют нулями, получая тем самым вектор $\widetilde{v}$. Находятся компоненты $S_0, S_1, \ldots, S_{2t+s-1}$ синдромного вектора $\widetilde{v}H^T$. Если они все равны нулю, то возвращается вектор $\widetilde{v}$ и процедура окончена.

   Вычисляются значения локаторов стираний $X_{t+1} = \alpha_{i_{t+1}}, \ldots, X_{t+s} = \alpha_{i_{t+s}}$ на основе известных позиций стираний $i_{t+1}, \ldots, i_{t+s}$. Вычисляются коэффициенты модифицированного синдромного многочлена $\widetilde{S}(x)$ (если $s = 0$, то $\widetilde{S}(x) = S(x)$).

2. На вход алгоритма 1 подается последовательность $\widetilde{S}_s$, $\widetilde{S}_{s+1}, \ldots$, $\widetilde{S}_{s+2t-1}$. На выходе данного алгоритма получается многочлен $\sigma(x)$. Пусть $l = \deg \sigma(x)$.

3. Если $l > 0$, то отыскиваются l корней многочлена $\sigma(x)$ последовательной подстановкой в него ненулевых элементов поля F. При этом локаторы ошибок — это величины, обратные корням многочлена $\sigma(x)$.

4. При вычислении значений ошибок выполняется один из следующих пунктов.

   4.1. Если среди локаторов стираний $X_{t+1}, \ldots, X_{t+s}$ имеется нулевое значение (в противном случае переходим в пункт 4.2), скажем, $X_p = 0$, то пусть:

   $$M = \{1, \ldots, l\} \cup \{t + 1, \ldots, t + s\} \backslash \{p\}.$$

   Находятся Z_j, $j \in M$, например, с помощью формул Форни для ОРС кодов:

   $$Z_j = \frac{\widetilde{\omega}(X_j^{-1})}{\prod\limits_{i \in M \backslash \{j\}} (1 - X_i X_j^{-1})}, \quad j \in M. \tag{21}$$

   После этого находятся значения ошибок $Y_j = Z_j / w_{i_j}$, $j \in M$. У вектора $\widetilde{v}$ из i_j-го символа, $X_j = \alpha_{i_j}$, вычитается значение Y_j, $j \in M$. При этом получается вектор $\widetilde{u}$. Пусть для некоторого i выполнено $\alpha_i = 0$. Вычисляется значение Z_p, равное скалярному произведению вектора $\widetilde{u}$ на первую строку матрицы H. Вычисляется значение ошибки $Y_p = Z_p / w_i$. Осталось в векторе $\widetilde{u}$ из i-го символа вычесть Y_p.

   4.2. Если условие 4.1 не выполнено, то пусть:

   $$M = \{1, \ldots, l\} \cup \{t + 1, \ldots, t + s\}.$$

   По формуле (21) находятся значения Z_j, затем значения ошибок $Y_j = Z_j / w_{i_j}$, $j \in M$. У вектора $\widetilde{v}$ из i_j-го символа, $X_j = \alpha_{i_j}$, вычитается значение Y_j, $j \in M$. При этом получается вектор $\widetilde{u}$.

   Если $\alpha_i = 0$ для некоторого i и $\deg \sigma(x) < L$, то вычисляется значение Z_0, равное скалярному произведению вектора $\widetilde{u}$ на первую строку матрицы H, а затем вычисляется значение ошибки $Y_0 = Z_0 / w_i$. Осталось в векторе $\widetilde{u}$ из i-го символа вычесть Y_0.

7. Декодирование кодов Гоппы с использованием алгоритма Берлекэмпа — Месси

Определение кода Гоппы опирается на два объекта: многочлен $G(x)$ с коэффициентами из поля $GF(q^m)$, который называется многочленом Гоппы; подмножество $L = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ элементов поля $GF(q^m)$, таких, что $G(\alpha_i) \neq 0$ для всех $\alpha_i \in L$. Код Гоппы $\Gamma(L, G)$ состоит из всех векторов $u = (u_0, u_1, \ldots, u_{n-1})$ с компонентами из $GF(q)$, для которых

$$R_u = \sum_{i=0}^{n-1} \frac{u_i}{x - \alpha_i} \equiv 0 \pmod{G(x)}.$$

Если $G(x)$ неприводим, то код $\Gamma(L, G)$ называется неприводимым кодом Гоппы. Множество L называется множеством нумераторов позиций кодового слова. Имеют место следующие оценки параметров для кодов Гоппы (см., напр., [9]).

Теорема 7. Параметры $[n,k,d]$-кода $\Gamma(L,G)$ над полем $GF(q)$, где $L \subseteq GF(q^m)$, связаны соотношением

$$n = |L|, \quad k \geqslant n - mr, \ r = \deg G(x), \quad d \geqslant r+1.$$

Нам понадобится следующее утверждение (см., напр., [1]).

Теорема 8. Код $\Gamma(L,G)$ представляет собой ограничение кода $GRS_{n-r}(L,y)$ на подполе $F = GF(q)$: $\Gamma(L,G) = GRS_{n-r}(L,y) \cap F^n$, где $r = \deg G(x)$, $y = (y_0, y_1, \ldots, y_{n-1})$,

$$y_i = G(\alpha_i) \prod_{j \neq i} \frac{1}{\alpha_i - \alpha_j}, \quad i = 0, 1, \ldots, n-1. \tag{22}$$

Следствие 3. Проверочная матрица кода $GRS_{n-r}(L,y)$, который задает код $\Gamma(L,G)$, имеет вид

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_0 & \alpha_1 & \ldots & \alpha_{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_0^{r-1} & \alpha_1^{r-1} & \ldots & \alpha_{n-1}^{r-1} \end{pmatrix} \begin{pmatrix} G(\alpha_0)^{-1} & 0 & \ldots & 0 \\ 0 & G(\alpha_1)^{-1} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & G(\alpha_{n-1})^{-1} \end{pmatrix},$$

т. е. совпадает с проверочной матрицей кода $\Gamma(L,G)$.

Таким образом, код $\Gamma(L,G)$ можно задать с помощью обобщенного кода Рида — Соломона.

Пусть код $\Gamma(L,G)$ является двоичным. Если $G(x)$ не имеет кратных корней, то код $\Gamma(L,G)$ называется сепарабельным кодом Гоппы. Пусть $\overline{G}(x)$ — полный квадрат некоторого многочлена над $GF(2^m)$ наименьшей степени, делящийся на $G(x)$. В случае сепарабельного кода $\overline{G}(x) = G^2(x)$. Для минимального расстояния сепарабельного кода $\Gamma(L,G)$ верна оценка $d \geqslant 2r+1$ и выполнено равенство $\Gamma(L,G) = \Gamma(L,\overline{G})$ (см., напр., [9]). Эти факты позволяют строить сепарабельный код $\Gamma(L,G) = \Gamma(L,\overline{G})$, а некоторые алгоритмы декодирования кодов Гоппы применять относительно кода $GRS_{n-2r}(\alpha,y)$, $r = \deg G(x)$.

Пусть $[n,k,d]$-код $\Gamma(L,G)$ задается на основе ОРС кода: $\Gamma(L,G) = GRS_{n-r}(L,y) \cap F^n$, $F = GF(q)$, $r = \deg G(x)$, $\widetilde{k} = n - r$ — размерность кода $GRS_{n-r}(L,y)$ длины n, $\overline{H}$ — проверочная матрица кода $GRS_{n-r}(L,y)$. Пусть $d, \widetilde{d}$ — кодовые расстояния кодов $\Gamma(L,G)$ и $GRS_{n-r}(L,y)$ соответственно. Так как $d \geqslant r+1$, $\widetilde{d} = n - \widetilde{k} + 1 = r+1$, то если в кодовом векторе $u \in \Gamma(L,G)$ произошло t ошибок и s стираний, причем $r \geqslant 2t+s$, то для его декодирования можно применять алгоритмы декодирования для ОРС-кодов.

Если же код $\Gamma(L,G)$ двоичный и сепарабельный, то $\Gamma(L,G) = GRS_{n-2r}(L,y) \cap F^n$, $F = GF(2)$, $\widetilde{k} = n - 2r$ — размерность кода $GRS_{n-2r}(L,y)$, $\overline{H}$ — проверочная матрица кода $GRS_{n-2r}(L,y)$. Также $d \geqslant 2r+1$, $\Gamma(L,G^2) \subseteq GRS_{n-2r}(L,y)$, $\widetilde{d} = 2r+1$, поэтому в этом случае алгоритмы декодирования для ОРС-кодов можно применять для декодирования вектора u, в котором t ошибок и s стираний, причем $2r \geqslant 2t+s$.

Алгоритм 7. (декодирование кода Гоппы на основе алгоритма Берлекэмпа — Месси на случай ошибок и стираний)

Вход: принятый вектор v.

Выход: исходный кодовый вектор u, в котором произошло s стираний и не более t ошибок, если $r \geqslant 2t+s$, $r = \deg G(x)$, $u \in \Gamma(L,G) \subseteq GRS_{n-r}(L,y)$ (для двоичного сепарабельного кода $2r \geqslant 2t+s$, $u \in \Gamma(L,G) \subseteq GRS_{n-2r}(L,y)$).

1. Определяется $t = [(r-s)/2]$ ($t = [(2r-s)/2]$ в случае двоичного сепарабельного кода Гоппы). В векторе v все стирания заменяют нулями, получая тем самым вектор $\widetilde{v}$. Находятся компоненты $S_0, S_1, \ldots, S_{2t+s-1}$ синдромного вектора $\widetilde{v}\overline{H}^T$. Если они все равны нулю, то возвращается вектор $\widetilde{v}$ и процедура окончена.

   Вычисляются значения локаторов стираний $X_{t+1} = \alpha_{i_{t+1}}, \ldots, X_{t+s} = \alpha_{i_{t+s}}$ на основе известных позиций стираний $i_{t+1}, \ldots, i_{t+s}$. Вычисляются коэффициенты модифицированного синдромного многочлена $\widetilde{S}(x)$ (если $s = 0$, то $\widetilde{S}(x) = S(x)$).

2. На вход алгоритма 1 подается последовательность $\widetilde{S}_s$, $\widetilde{S}_{s+1}, \ldots$, $\widetilde{S}_{s+2t-1}$. На выходе данного алгоритма получается многочлен $\sigma(x)$. Пусть $l = \deg \sigma(x)$.

3. Отыскиваются l корней многочлена $\sigma(x)$ последовательной подстановкой в него ненулевых элементов поля $GF(q^m)$. При этом локаторы ошибок — это величины, обратные корням многочлена $\sigma(x)$.

4. При вычислении значений ошибок выполняется один из следующих пунктов.

   4.1. Если среди локаторов стираний $X_{t+1}, \ldots, X_{t+s}$ имеется нулевое значение (в противном случае переходим в пункт 4.2), скажем, $X_p = 0$, то пусть
   $$M = \{1, \ldots, l\} \cup \{t+1, \ldots, t+s\} \backslash \{p\}$$
   — множество индексов локаторов ошибок и стираний без учета индекса p. Находятся Z_j, $j \in M$, например, с помощью алгоритма Форни (21) для обобщенных кодов РС. После этого находятся значения ошибок $Y_j = Z_j G(X_j)$, $j \in M$. У вектора $\widetilde{v}$ из i_j-го символа, $X_j = \alpha_{i_j}$, вычитается значение Y_j, $j \in M$. При этом получается вектор $\widetilde{u}$. Пусть для некоторого i выполнено $\alpha_i = 0$ (в противном случае все локаторы стираний были бы ненулевые). Вычисляется значение Z_p, равное скалярному произведению вектора $\widetilde{u}$ на первую строку матрицы $\overline{H}$. Вычисляется значение ошибки $Y_p = Z_p G(\alpha_i)$. Осталось в векторе $\widetilde{u}$ из i-го символа вычесть Y_p.

   4.2. Если условие 4.1 не выполнено, то пусть $M = \{1, \ldots, l\} \cup \{t+1, \ldots, t+s\}$. По формуле (21) находятся значения Z_j, затем — значения ошибок $Y_j = Z_j G(X_j)$, $j \in M$. У вектора $\widetilde{v}$ из i_j-го символа, $X_j = \alpha_{i_j}$, вычитается значение Y_j, $j \in M$. При этом получается вектор $\widetilde{u}$.
   Если $\alpha_i = 0$ для некоторого i и $\deg \sigma(x)$ строго меньше длины LFSR (полученного на выходе алгоритма 1), то вычисляется значение Z_0, равное скалярному произведению вектора $\widetilde{u}$ на первую строку матрицы $\overline{H}$, а затем вычисляется значение ошибки $Y_0 = Z_0 G(\alpha_i)$. Осталось в векторе $\widetilde{u}$ из i-го символа вычесть Y_0.

Пример 3. Рассмотрим расширение поля $GF(2) \subset GF(2^4)$, где поле $GF(2^4)$ строится на основе примитивного многочлена $p(x) = x^4 + x + 1$ и рассматривалось в примере 1. Пусть $L = GF(2^4) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\}$, $G(x) = x^2 + x + \alpha^3$. Так как след элемента α^3 в поле $GF(2^4)$ не равен нулю, то многочлен $G(x)$ в этом поле не имеет корней. Поэтому из неприводимости $G(x)$ над $GF(2^4)$ следует, что код $\Gamma(L, G)$ является сепарабельным, поэтому он может исправлять до двух ошибок, либо одну ошибку и до двух стираний, либо до четырех стираний. Проверочная матрица H кода $\Gamma(L, G)$ примет такой вид:
$$H = \begin{pmatrix} G(0)^{-1} & G(1)^{-1} & G(\alpha)^{-1} & \ldots & G(\alpha^{14})^{-1} \\ 0G(0)^{-1} & 1G(1)^{-1} & \alpha G(\alpha)^{-1} & \ldots & \alpha^{14} G(\alpha^{14})^{-1} \end{pmatrix} =$$
$$= \begin{pmatrix} \alpha^{12} & \alpha^{12} & \alpha^4 & \alpha^3 & \alpha^9 & \alpha^4 & \alpha & \alpha^8 & \alpha^6 & \alpha^3 & \alpha^6 & \alpha & \alpha^2 & \alpha^2 & \alpha^8 & \alpha^9 \\ 0 & \alpha^{12} & \alpha^5 & \alpha^5 & \alpha^{12} & \alpha^8 & \alpha^6 & \alpha^{14} & \alpha^{13} & \alpha^{11} & 1 & \alpha^{11} & \alpha^{13} & \alpha^{14} & \alpha^6 & \alpha^8 \end{pmatrix} =$$
$$= \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$
Так как все строки матрицы H линейно независимы, то $n - k = 8$, $k = 8$. Выписав построчно фундаментальную систему решений системы однородных линейных уравнений $HX = O$, находим порождающую матрицу кода $\Gamma(L, G)$:
$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

В данном случае $\Gamma(L, G) \subseteq GRS_{12}(L, y)$, при этом проверочная матрица $\overline{H}$ кода $GRS_{12}(L, y)$, учитывая следствие 3, имеет вид
$$\overline{H} = \begin{pmatrix} \alpha^9 & \alpha^9 & \alpha^8 & \alpha^6 & \alpha^3 & \alpha^8 & \alpha^2 & \alpha & \alpha^{12} & \alpha^6 & \alpha^{12} & \alpha^2 & \alpha^4 & \alpha^4 & \alpha & \alpha^3 \\ 0 & \alpha^9 & \alpha^9 & \alpha^8 & \alpha^6 & \alpha^{12} & \alpha^7 & \alpha^7 & \alpha^4 & \alpha^{14} & \alpha^6 & \alpha^{12} & 1 & \alpha & \alpha^{14} & \alpha^2 \\ 0 & \alpha^9 & \alpha^{10} & \alpha^{10} & \alpha^9 & \alpha & \alpha^{12} & \alpha^{13} & \alpha^{11} & \alpha^7 & 1 & \alpha^7 & \alpha^{11} & \alpha^{13} & \alpha^{12} & \alpha \\ 0 & \alpha^9 & \alpha^{11} & \alpha^{12} & \alpha^{12} & \alpha^5 & \alpha^2 & \alpha^4 & \alpha^3 & 1 & \alpha^9 & \alpha^2 & \alpha^7 & \alpha^{10} & \alpha^{10} & 1 \end{pmatrix}.$$

Пусть на приемном конце получен вектор:

$$v = (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1),$$

в котором до двух ошибок (как видно, стирающих символов в принятом векторе нет).

Для декодирования принятого вектора применим алгоритм 7.

1. Определяем $s = 0$, $t = \deg G(x) = 2$. Находим синдромный вектор $S = v\overline{H}^T = \begin{pmatrix} \alpha^9, & \alpha^9, & \alpha^{10}, & \alpha^6 \end{pmatrix}$.

2. Применяя к данной последовательности алгоритм Берлекэмпа — Месси 1, получаем $\sigma(x) = 1 + \alpha^2 x + \alpha^9 x^2$.

3. Корнями многочлена $\sigma(x)$ являются $x_1 = \alpha^{12}$, $x_2 = \alpha^9$, поэтому $X_1 = x_1^{-1} = \alpha^3 = \alpha_4$, $X_2 = x_2^{-1} = \alpha^6 = \alpha_7$. Следовательно, ошибки произошли на 4-й и 7-й позициях.

4. Так как код двоичный, то исходный кодовый вектор равен:

$$u = (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1),$$

при этом длина LFSR совпадает с $\deg \sigma(x)$, поэтому на позиции с номером 0 ошибок нет.

Литература

[1] Блейхут Р. Теория и практика кодов, контролирующих ошибки. Пер. с англ. Москва: Мир, 1986. 576 с. URL: http://publ.lib.ru/ARCHIVES/B/BLEYHUT_Richard_E/_Bleyhut_R.E..html

[2] Huffman W. Cary. Fundamentals of Error-Correcting Codes. Cambridge: Cambridge University Press, 2003. 646 p. DOI: https://doi.org/10.1017/CBO9780511807077.

[3] Gao S. A new algorithm for decoding Reed–Solomon codes // In: Bhargava V.K., Poor H.V., Tarokh V., Yoon S. (eds.) Communications, Information and Network Security. The Springer International Series in Engineering and Computer Science (Communications and Information Theory), vol 712, pp. 55–68. Springer, Boston, MA. DOI: https://doi.org/10.1007/978-1-4757-3789-9_5.

[4] Massey J.L. Shift-register synthesis and BCH decoding // IEEE Transactions on Information Theory. 1969. Vol. IT. 15, № 1. P. 122–127. DOI: https://doi.org/10.1109/TIT.1969.1054260.

[5] Sugiyama Y. et al. A method for solving key equation for decoding Goppa codes // Information and Control. 1975. Vol. 27. Issue 1. P. 87–99. DOI: https://doi.org/10.1016/S0019-9958(75)90090-X

[6] Dornstetter J.L. On the equivalence Between Berlekamp's and Euclid's Algorithm // IEEE Trans. Inform. Theory. 1987. Vol. IT-33, № 3. P. 428–431.

[7] Рацеев С.М., Череватенко О.И. Об алгоритмах декодирования обобщенных кодов Рида — Соломона на случай ошибок и стираний // Вестник Самарского университета. Естественнонаучная серия. 2020. Т. 26, № 3. С. 17–29. DOI: https://doi.org/10.18287/2541-7525-2020-26-3-17-29.

[8] Рацеев С.М., Череватенко О.И. Об алгоритмах декодирования обобщенных кодов Рида — Соломона на случай ошибок и стираний. II // Вестник Самарского университета. Естественнонаучная серия. 2021. Т. 27, № 2 (в печати).

[9] Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки: пер. с англ. Москва: Связь, 1979. 744 с. URL: https://ru.djvu.online/file/jZGJCUDSUc4AZ.

Scientific article

DOI: 10.18287/2541-7525-2021-27-1-44-61

Submited: 10.01.2021
Revised: 17.02.2021
Accepted: 28.02.2021

S.M. Ratseev
Ulyanovsk State University, Ulyanovsk, Russian Federation
E-mail: ratseevsm@mail.ru. ORCID: https://orcid.org/0000-0003-4995-9418
A.D. Lavrinenko
Ulyanovsk State University, Ulyanovsk, Russian Federation
E-mail: anutalavrinenko@gmail.com. ORCID: https://orcid.org/0000-0003-3652-1097
E.A. Stepanova
Ulyanovsk State University, Ulyanovsk, Russian Federation
E-mail: kate_stepanova@bk.ru. ORCID: https://orcid.org/0000-0003-0276-1615

ON THE BERLEKAMP — MASSEY ALGORITHM AND ITS APPLICATION FOR DECODING ALGORITHMS

ABSTRACT

The paper is devoted to the Berlekamp — Masssey algorithm and its equivalent version based on the extended Euclidean algorithm. An optimized Berlekamp — Massey algorithm is also given for the case of a field of characteristic 2. The Berlekamp — Massey algorithm has a quadratic complexity and is used, for example, to solve systems of linear equations in which the matrix of the system is the Toeplitz matrix. In particular, such systems of equations appear in algorithms for the syndrome decoding of BCH codes, Reed — Solomon codes, generalized Reed — Solomon codes, and Goppa codes. Algorithms for decoding the listed codes based on the Berlekamp — Massey algorithm are given.

Key words: Berlekamp — Massey algorithm; extended Euclidean algorithm; Reed — Solomon codes; code decoding.

Citation. Ratseev S.M., Lavrinenko A.D., Stepanova E.A. On the Berlekamp — Massey algorithm and its application for decoding algorithms. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2021, vol. 27, no. 1, pp. 44–61. DOI: http://doi.org/10.18287/2541-7525-2021-27-1-44-61. (In Russ.)

Information about the conflict of interests: authors and reviewers declare no conflict of interests.

© Ratseev S.M., 2021
Sergey Mihaylovich Ratseev — Doctor of Physical and Mathematical Sciences, associate professor, Department of Information Security and Control Theory, Ulyanovsk State University, 42, Leo Tolstoy Street, Ulyanovsk, 432017, Russian Federation.
© Lavrinenko A.D., 2021
Anna Dmitrievna Lavrinenko — student of the Department of Information Security and Control Theory, Ulyanovsk State University, 42, Leo Tolstoy Street, Ulyanovsk, 432017, Russian Federation.
© Stepanova E.A., 2021
Ekaterina Alekseevna Stepanova — student of the Department of Information Security and Control Theory, Ulyanovsk State University, 42, Leo Tolstoy Street, Ulyanovsk, 432017, Russian Federation.

References

[1] Blahut Richard E. Theory and practice of error control codes. Translation from English. Moscow: Mir, 1986, 576 p. Available at: https://scask.ru/h_book_tpc.php. (In Russ.)

[2] Huffman W. Cary. Fundamentals of Error-Correcting Codes. Cambridge: Cambridge University Press, 2003, 646 p. DOI: https://doi.org/10.1017/CBO9780511807077.

[3] Gao S. A new algorithm for decoding Reed—Solomon codes. In: Bhargava V.K., Poor H.V., Tarokh V., Yoon S. (eds.) Communications, Information and Network Security. The Springer International Series in Engineering and Computer Science (Communications and Information Theory), vol. 712, pp. 55–68. Springer, Boston, MA. DOI: https://doi.org/10.1007/978-1-4757-3789-9_5.

[4] Massey J.L. Shift-register synthesis and BCH decoding. *IEEE Transactions on Information Theory*, 1969, vol. IT. 15, issue 1, pp. 122–127. DOI: https://doi.org/10.1109/TIT.1969.1054260.

[5] Sugiyama Y. et al. A method for solving key equation for decoding Goppa codes. *Information and Control*, 1975, vol. 27, issue 1, pp. 87–99. DOI: https://doi.org/10.1016/S0019-9958(75)90090-X.

[6] Dornstetter J.L. On the equivalence Between Berlekamp's and Euclid's Algorithm. *IEEE Transactions on Information Theory*, 1987, vol. IT-33, issue 3, pp. 428–431. DOI: https://doi.org/10.1109/TIT.1987.1057299.

[7] Ratseev S.M., Cherevatenko O.I. On decoding algorithms for generalized Reed-Solomon codes with errors and erasures. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2020, vol. 26, no. 3, pp. 17–29. DOI: https://doi.org/10.18287/2541-7525-2020-26-3-17-29. (In Russ.)

[8] Ratseev S.M., Cherevatenko O.I. On decoding algorithms for generalized Reed-Solomon codes with errors and erasures. II. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series.* 2021, vol. 27, no. 2. (Print, in Russ.)

[9] Mac Williams F.J., Sloane N.J.A. The theory of error correcting codes. Moscow: Svyaz', 1979, 744 p. Available at: https://ru.djvu.online/file/jZGJCUDSUc4AZ. (In Russ.)

Научная статья
DOI: 10.18287/2541-7525-2021-27-1-62-73

УДК 519.7

Дата: поступления статьи: 11.12.2020
после рецензирования: 20.01.2021
принятия статьи: 28.02.2021

С.М. Рацеев
Ульяновский государственный университет,
г. Ульяновск, Российская Федерация
E-mail: ratseevsm@mail.ru. ORCID: https://orcid.org/0000-0003-4995-9418
О.И. Череватенко
Ульяновский государственный педагогический университет
имени И.Н. Ульянова, г. Ульяновск, Российская Федерация
E-mail: choi2008@mail.ru. ORCID: https://orcid.org/0000-0003-3931-9425
В.А. Чернявская
Ульяновский государственный педагогический университет
имени И.Н. Ульянова, г. Ульяновск, Российская Федерация
E-mail: vera.chernya@yandex.ru. ORCID: https://orcid.org/0000-0001-9875-2232

О НЕКОТОРЫХ КРИПТОСИСТЕМАХ, ОСНОВАННЫХ НА АЛГЕБРАИЧЕСКИХ КОДАХ

АННОТАЦИЯ

В 1978 г. Мак-Элис построил первую кодовую криптосистему с открытым ключом, которая основана на применении помехоустойчивых кодов. При этом эффективные атаки на секретные ключи этой криптосистемы до сих пор не найдены. В работе приводятся описания классической и модернизированной криптосистем Мак-Элиса и Нидеррайтера, а также примеры их практического применения на основе кодов Гоппы с использованием алгоритма Паттерсона. Также приводятся алгоритмы двухшаговых протоколов аутентификации с нулевым разглашением на основе кодовых криптосистем.

Ключевые слова: криптосистема Мак-Элиса; помехоустойчивые коды; коды Гоппы; декодирование кода.

Цитирование. Рацеев С.М., Череватенко О.И., Чернявская В.А. О некоторых криптосистемах, основанных на алгебраических кодах // Вестник Самарского университета. Естественнонаучная серия. 2021. Т. 27, № 1. С. 62–73. DOI: http://doi.org/10.18287/2541-7525-2021-27-1-62-73.

Информация о конфликте интересов: авторы и рецензенты заявляют об отсутствии конфликта интересов.

© Рацеев С.М., 2021
Сергей Михайлович Рацеев — доктор физико-математических наук, доцент, профессор кафедры информационной безопасности и теории управления, Ульяновский государственный университет, 432017, Российская Федерация, г. Ульяновск, ул. Льва Толстого, 42.

© Череватенко О.И., 2021
Ольга Ивановна Череватенко — кандидат физико-математических наук, доцент, доцент кафедры высшей математики, Ульяновский государственный педагогический университет имени И.Н. Ульянова, 432071, Российская Федерация, г. Ульяновск, пл. Ленина, 4/5.

© Чернявская В.А., 2021
Вера Алексеевна Чернявская — студент кафедры информационной безопасности и теории управления, Ульяновский государственный университет, 432017, Российская Федерация, г. Ульяновск, ул. Льва Толстого, 42.

Введение

В 1978 г. Мак-Элисом предложена первая криптосистема, основанная на алгебраических блоковых кодах [1]. В ее основе лежит маскировка быстрого алгоритма декодирования посредством умножения исходной порождающей матрицы G на случайную невырожденную матрицу, которая, в частности, является секретным ключом криптосистемы. Полученный результат (открытый ключ) представляет собой порождающую матрицу, имеющую вид случайно выбранных линейно независимых векторов. Злоумышленник, имеющий только открытый ключ, вынужден использовать сложный алгоритм неалгебраического декодирования (NP-полная задача). Законный пользователь, знающий секретный ключ, снимает действие маскировки и применяет быстрый алгебраический алгоритм декодирования (полиномиально разрешимая задача). Данная криптосистема на данный момент остается криптостойкой, так как нет ни одного эффективного алгоритма нахождения секретного ключа. Более того, данная криптосистема является одним из претендентов на официальную постквантовую криптосистему [2].

Криптосистема Мак-Элиса при использовании кодов Гоппы считается криптостойкой. Для декодирования кодов Гоппы хорошо известен алгоритм Паттерсона [3]. Но он применим только для двоичных кодов Гоппы. При этом заметим, что любой алгоритм декодирования обобщенных кодов Рида — Соломона можно применить и для кодов Гоппы над любым полем. Для обобщенных кодов Рида — Соломона и кодов Гоппы подобные алгоритмы рассматривались в работах [4–7].

1. Криптосистема Мак-Элиса

Классическая криптосистема. Пусть G — порождающая матрица $[n, k, d]$-кода над $GF(q)$, исправляющего t и менее ошибок (в оригинальной статье предлагается использовать двоичные сепарабельные коды Гоппы), C — невырожденная матрица порядка k над полем $GF(q)$, P и D — перестановочная и диагональная матрицы порядка n соответственно (для двоичных кодов матрица D не используется).

Матрица $\widetilde{G} = C \cdot G \cdot P \cdot D$ является открытым ключом абонента A, как и параметры n, k, t. Маскирующие матрицы C, P, D и порождающая матрица G являются секретным ключом абонента A. В силу того, что матрицы C, P, D невырождены, матрица $\widetilde{G}$ является порождающей матрицей эквивалентного кода. Предположим, что абонент B хочет передать абоненту A сообщение x длины k с компонентами из $GF(q)$. Алгоритм шифрования, предложенный Мак-Элисом, выглядит следующим образом.

1. Случайным равновероятным образом генерируется вектор ошибок e длины n над $GF(q)$ веса не более t.

2. Абонент B вычисляет шифрованное сообщение $y = x\widetilde{G} + e$, которое по открытому каналу связи передает абоненту A.

Вектор ошибок e, генерируемый на первом шаге, является случайным параметром шифра, который значительно усложняет криптоанализ. При $wt(e) = t$ сложность дешифрования будет максимальной. Также заметим, что при каждом таком шифровании вектор e должен генерироваться заново. Для расшифрования сообщения абонент A совершает следующие действия.

1. Умножение полученного вектора на матрицу $(PD)^{-1}$: $\widetilde{y} = yD^{-1}P^{-1}$. При этом $\widetilde{y} = yD^{-1}P^{-1} = = xCG + \widetilde{e} = \widetilde{x}G + \widetilde{e}$, где $\widetilde{x} = xC$, $wt(\widetilde{e}) = wt(e)$.

2. Декодирование вектора $\widetilde{x}$ на основе вектора $\widetilde{y}$, т. е. получение вектора $\widetilde{x} = xC$.

3. Нахождение исходного сообщения x путем умножения вектора $\widetilde{x}$ на C^{-1}: $x = \widetilde{x}C^{-1}$.

Замечание 1. Пусть G и H — порождающая и проверочная матрицы некоторого линейного кода, C и D — невырожденные квадратные матрицы подходящих размеров (для вычисления CG, DH). Порождающие матрицы CG и G задают один и тот же линейный код, так как $GH^T = O$, тогда и только тогда, когда $CGH^T = O$. Аналогично проверочные матрицы H и DH задают один и тот же линейный код. Это значит, что для декодирования вектора $\widetilde{x}$ на втором шаге приведенного выше алгоритма применяется проверочная матрица H (если она необходима), соответствующая матрице G.

Модернизированная криптосистема. Для того чтобы уменьшить объем параметров криптосистемы Мак-Элиса, имеется модернизированная версия данной криптосистемы [8], которая использует порождающую матрицу G в канонической форме: $G = (I_k, Q_{k\times(n-k)})$. В этом случае вместо хранения $k \times n$ элементов достаточно хранить только матрицу Q размера $k \times (n-k)$. Более того, для

алгоритмов кодирования и декодирования требуется меньшее число операций. Также вместо матриц C, P, D в качестве секретного ключа хранится только перестановка элементов множества L и многочлен $G(x)$ кода $\Gamma(L, G)$.

Как утверждается в работе [8], криптостойкость модернизированной версии эквивалентна криптостойкости классической версии криптосистемы Мак-Элиса. Итак, сначала вычисляется открытый ключ G криптосистемы на основе параметров q, m, n, r.

1. Случайным образом генерируется многочлен $G(x)$ степени r над полем $GF(q^m)$ (например, можно сгенерировать неприводимый многочлен).

2. Случайным образом выбираются n элементов поля $GF(q^m)$, не являющиеся корнями многочлена $G(x)$, которые определяют множество L. Если $G(x)$ неприводим, то можно взять любые различные n элементов поля $GF(q^m)$.

3. Вычисляется проверочная матрица H' над полем $GF(q^m)$ размера $r \times n$ на основе L и $G(x)$, $r = \deg G(x)$.

4. С помощью элементарных преобразований строк матрица H' приводится к систематическому виду CH' (некоторые столбцы такой матрицы образуют единичную матрицу, а невырожденная матрица C является произведением соответствующих матриц элементарных преобразований), а затем с помощью перестановки столбцов приводится к виду $H = (Q^T_{(n-k)\times k}, I_{n-k})$, т. е. матрица CH' справа умножается на перестановочную матрицу P: $H = CH'P$. К множеству L применяется такая же перестановка (обозначение L оставим прежним).

5. На основе матрицы H вычисляется порождающая матрица G в канонической форме: $G = (I_k, Q_{k\times(n-k)})$.

В итоге матрица G является открытым ключом криптосистемы. Как видно из алгоритма, для получения H требуется некоторая невырожденная матрица C и перестановочная матрица P. Заметим, что если $n = q^m$, то $L = GF(q^m)$. Также в качестве $G(x)$ чаще всего выбирают неприводимый многочлен над $GF(q^m)$. Множество L для данной криптосистемы является случайным и держится в секрете. Алгоритм шифрования в модернизированной версии не отличатся от классической, разве что на него требуется меньшее число операций. Для того чтобы абоненту B передать абоненту A сообщение x длины k с компонентами из $GF(q)$, требуется выполнить следующие шаги.

1. Абонент B случайным равновероятным образом генерирует вектор ошибок e длины n над $GF(q)$ веса не более t.

2. Абонент B получает шифрованное сообщение $y = xG + e = x(I, Q) + e = (x, xQ) + e$, которое по открытому каналу связи передает абоненту A.

Для расшифрования сообщения абонент A совершает следующие действия.

1. По вектору y вычисляется синдромный вектор S (синдромный многочлен $S(x)$).

2. С помощью алгоритма декодирования полиномиальной сложности находится вектор e веса не более t, который имеет синдром S.

3. После этого вычисляется кодовый вектор $u = y - e$, из которого извлекается сообщение x (из первых k позиций вектора u).

Есть несколько оснований для использования кодов Гоппы в криптосистеме Мак-Элиса: 1) существуют быстрые алгоритмы полиномиальной сложности декодирования кодов Гоппы; 2) код Гоппы легко генерировать, но очень сложно обнаружить «замаскированный» код Гоппы; 3) код Гоппы можно построить с помощью любого неприводимого многочлена над $GF(2^m)$, при этом порождающая матрица кода будет иметь «почти случайный» вид.

Заметим, что для любой фиксированной длины n существует «очень много» различных кодов Гоппы. Пусть $N(q, s, r)$ — число неэквивалентных неприводимых кодов Гоппы над полем $GF(q)$ длины q^s и степени r многочлена $G(x)$. Точной формулы для $N(q, s, r)$ пока неизвестно. В работе [9] приводятся верхние границы для $N(q, s, r)$, которые являются точными для некоторых небольших значений параметров. Например, число двоичных неприводимых кодов Гоппы длины $n = 128$ и степенью неприводимого многочлена $r = 10$ оценивается сверху числом $N(2, 7, 10) = 1037499670492467 > 10^{15}$. А для числа $N(2, 7, 15)$ (т. е. для кодов той же длины 128 с неприводимым многочленом $G(x)$ степени 15) уже выполнено равенство $N(2, 7, 15) = 2376547806952061120164378 1 > 2 \cdot 10^{25}$. Если увеличить длину

кодов до $n = 4096$ (чтобы обеспечивался должный уровень криптостойкости системы Мак-Элиса), то для данной границы уже при $r = 7$ получаем $N(2, 12, 7) = 13728607731106143 > 10^{16}$.

Заметим, что криптосистема Мак-Элиса требует очень большого объема памяти для своих параметров. Для примера, чтобы добиться 80-битной криптостойкости, для алгоритма RSA необходим 1024-битный ключ, при этом для криптосистемы Мак-Элиса требуется ключ размера не менее 450 кбит для достижения той же степени криптостойкости.

Пример 1 (классическая криптосистема Мак-Элиса). Рассмотрим расширение поля $GF(2) \subset GF(2^4)$. Пусть поле $GF(2^4)$ строится на основе примитивного многочлена $p(x) = x^4 + x + 1$, α — примитивный элемент поля $GF(2^4)$:

$$\begin{array}{rcccccrcccccl}
\alpha^0 = & 1 & & & & = & 1000, & \alpha^1 = & & \alpha & & = & 0100, \\
\alpha^2 = & & & \alpha^2 & & = & 0010, & \alpha^3 = & & & \alpha^3 & = & 0001, \\
\alpha^4 = & 1 & +\alpha & & & = & 1100, & \alpha^5 = & & \alpha & +\alpha^2 & = & 0110, \\
\alpha^6 = & & & \alpha^2 & +\alpha^3 & = & 0011, & \alpha^7 = & 1 & +\alpha & +\alpha^3 & = & 1101, \\
\alpha^8 = & 1 & & +\alpha^2 & & = & 1010, & \alpha^9 = & & \alpha & +\alpha^3 & = & 0101, \\
\alpha^{10} = & 1 & +\alpha & +\alpha^2 & & = & 1110, & \alpha^{11} = & & \alpha & +\alpha^2 & +\alpha^3 & = & 0111, \\
\alpha^{12} = & 1 & +\alpha & +\alpha^2 & +\alpha^3 & = & 1111, & \alpha^{13} = & 1 & & +\alpha^2 & +\alpha^3 & = & 1011, \\
\alpha^{14} = & 1 & & & +\alpha^3 & = & 1001, & \alpha^{15} = & 1 & & & & = & 1000.
\end{array}$$

Пусть $L = GF(2^4) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\}$, $G(x) = x^2 + x + \alpha^3$. Так как след элемента α^3 в поле $GF(2^4)$ не равен нулю, то многочлен $G(x)$ в этом поле не имеет корней. Поэтому из неприводимости $G(x)$ над $GF(2^4)$ следует, что код $\Gamma(L, G)$ является сепарабельным, т. е. он исправляет до двух ошибок. Проверочная матрица H кода $\Gamma(L, G)$ примет такой вид:

$$H = \begin{pmatrix} G(0)^{-1} & G(1)^{-1} & G(\alpha)^{-1} & \ldots & G(\alpha^{14})^{-1} \\ 0G(0)^{-1} & 1G(1)^{-1} & \alpha G(\alpha)^{-1} & \ldots & \alpha^{14}G(\alpha^{14})^{-1} \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha^{12} & \alpha^{12} & \alpha^4 & \alpha^3 & \alpha^9 & \alpha^4 & \alpha & \alpha^8 & \alpha^6 & \alpha^3 & \alpha^6 & \alpha & \alpha^2 & \alpha^2 & \alpha^8 & \alpha^9 \\ 0 & \alpha^{12} & \alpha^5 & \alpha^5 & \alpha^{12} & \alpha^8 & \alpha^6 & \alpha^{14} & \alpha^{13} & \alpha^{11} & 1 & \alpha^{11} & \alpha^{13} & \alpha^{14} & \alpha^6 & \alpha^8 \end{pmatrix} =$$

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

Так как все строки матрицы H линейно независимы, то $n - k = 8$, $k = 8$. Выписав построчно фундаментальную систему решений системы однородных линейных уравнений $HX = O$, находим порождающую матрицу кода $\Gamma(L, G)$:

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

Абонент A генерирует невырожденную матрицу C и перестановочную матрицу P:

$$C = \begin{pmatrix}
1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 0
\end{pmatrix}, \quad C^{-1} = \begin{pmatrix}
1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix},$$

$$P = \begin{pmatrix} e_{\sigma(0)} \\ e_{\sigma(1)} \\ \dots \\ e_{\sigma(15)} \end{pmatrix} = \begin{pmatrix}
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0
\end{pmatrix},$$

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 4 & 10 & 13 & 9 & 0 & 7 & 15 & 3 & 14 & 11 & 5 & 1 & 8 & 2 & 12 & 6 \end{pmatrix},$$

где σ — подстановка на множестве $\{0, 1, \dots, 15\}$ (строки и столбцы нумеруем с нуля). После этого абонент A вычисляет матрицу:

$$\widetilde{G} = CGP = \begin{pmatrix}
0&0&0&1&1&0&1&0&0&1&1&1&0&1&1&0\\
0&0&0&0&1&0&1&0&0&1&1&0&0&0&0&1\\
0&0&1&0&1&0&0&0&0&0&1&0&1&1&0&1\\
0&0&0&1&0&1&0&1&1&0&1&1&1&0&1&0\\
1&0&0&1&0&1&1&0&1&1&0&1&0&1&1&1\\
0&1&1&0&0&0&1&1&0&1&1&1&0&0&0&0\\
0&0&0&0&1&0&0&0&1&0&0&0&1&0&1&1\\
1&1&1&0&1&0&0&1&0&1&0&0&1&1&1&1
\end{pmatrix}.$$

Параметры $n = 16$, $k = 8$, $t = 2$ и матрица $\widetilde{G}$ являются открытым ключом абонента A.

Предположим, что абонент B хочет передать абоненту A сообщение $x = (0, 1, 1, 1, 0, 0, 1, 1)$, которое нужно предварительно зашифровать на открытом ключе абонента A. Абонент B генерирует вектор ошибок веса два и вычисляет:

$$y = x\widetilde{G} + (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) =$$

$$= (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0).$$

Сообщение y передается абоненту A по открытому каналу связи. Для расшифрования сообщения y абонент A проделывает следующие действия. Сначала вектор y умножается на $P^{-1} = P^T$:

$$\widetilde{y} = yP^{-1} = (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1),$$

т. е. элементы в векторе y переставляются в соответствии с перестановкой σ. Для декодирования $\widetilde{y}$ применим алгоритм Паттерсона (см. [3; 4]). По вектору $\widetilde{y}$ вычисляется синдромный многочлен

$$S(x) \equiv \sum_{i=0}^{15} \frac{\widetilde{y}_i}{x - \alpha_i} \equiv \frac{1}{x-1} + \frac{1}{x-\alpha^3} + \frac{1}{x-\alpha^4} + \frac{1}{x-\alpha^7} +$$

$$+ \frac{1}{x-\alpha^8} + \frac{1}{x-\alpha^9} + \frac{1}{x-\alpha^{10}} + \frac{1}{x-\alpha^{14}} \equiv \alpha^9 + \alpha^5 x \pmod{G(x)}.$$

Вычисляется $T(x) \equiv (\alpha^9 + \alpha^5 x)^{-1} \equiv 1 + \alpha^{14} x \pmod{G(x)}$.

Учитывая, что $s(x) \equiv \sqrt{x} \equiv \alpha^9 + x \pmod{G(x)}$, вычисляется $p(x)$:

$$p(x) \equiv \sqrt{T(x) + x} \equiv \sqrt{1 + \alpha^3 x} \equiv$$

$$\equiv (1)^8 + (\alpha^3)^8(\alpha^9 + x) \equiv \alpha^{14} + \alpha^9 x \pmod{G(x)}.$$

Полагается $r = \deg G(x) = 2$, $r_{-1}(x) = G(x)$, $r_0(x) = p(x)$, $v_{-1}(x) = 0$, $v_0(x) = 1$. При $j = 0$ выполнено:

$$\deg r_{-1}(x) = 2 > \frac{r}{2}, \quad \deg r_0(x) = \frac{r}{2},$$

поэтому с точностью до константы $\sigma(x) = r_0^2(x) + x v_0(x) = \alpha^{13} + x + \alpha^3 x^2$.

Корнями многочлена $\sigma(x)$ являются $X_1 = \alpha^4 = \alpha_5$, $X_2 = \alpha^6 = \alpha_7$, поэтому ошибки в векторе $\widetilde{y}$ содержатся на 5-й и 7-й позициях. После исправления двух ошибок в векторе $\widetilde{y}$ новый вектор примет вид

$$\overline{y} = (0,1,0,0,1,0,0,1,1,1,1,1,0,0,0,1) = xCG = \widetilde{x}G.$$

Так как столбцы матрицы G с номерами 7, 9–15 (нумеруя с нуля) образуют единичную матрицу, то из вектора $\overline{y}$ извлекаем вектор $\widetilde{x} = (1,1,1,1,0,0,0,1)$. Осталось вычислить:

$$x = \widetilde{x}C^{-1} = (0,1,1,1,0,0,1,1).$$

2. Криптосистема Нидеррайтера

Другим важным примером кодовых криптосистем является схема Нидеррайтера [10]. Открытым ключом в этой криптосистеме являются параметры n, k, t и матрица $\widetilde{H} = CHPD$, где H — проверочная матрица алгебраического $[n,k,d]$-кода над $GF(q)$ (в оригинальной статье предлагалось использовать обобщенные коды Рида — Соломона, но такой вариант взломан), C — невырожденная матрица порядка $n-k$ над полем $GF(q)$, P и D — перестановочная и диагональная матрицы порядка n соответственно (для двоичных кодов матрица D не используется). Маскирующие матрицы C, P, D и проверочная матрица H являются секретным ключом абонента A.

Предположим, что абонент B хочет передать абоненту A сообщение e длины n над $GF(q)$ веса не более t, т. е. сообщения в этом случае не являются кодовыми словами, а представляют собой всевозможные векторы ошибок, которые этот код в состоянии исправлять (как помещать открытые тесты в векторы-ошибок см., напр., [11]). Шифрованное сообщение длины $n-k$ получается следующим образом: $y = e\widetilde{H}^T$.

При этом наибольшая стойкость будет при $wt(e) = t$. Для расшифрования сообщения абонент A совершает следующие действия.

1. Абонент A умножает полученный вектор на $(C^T)^{-1}$:

$$S = y(C^T)^{-1} = eDP^TH^TC^T(C^T)^{-1} = eDP^TH^T = \widetilde{e}H^T,$$

где $\widetilde{e} = eDP^T$, $wt(\widetilde{e}) = wt(e)$.

2. В смежном классе с синдромом S теперь с помощью алгоритма декодирования вычисляется вектор ошибок $\widetilde{e}$ (здесь можно применить любой алгоритм декодирования, который по синдромному вектору находит вектор ошибок: алгоритм Сугиямы, Берлекэмпа — Месси и т. д.).

3. Нахождение исходного сообщения e путем умножения вектора $\widetilde{e}$ на PD^{-1}: $e = \widetilde{e}PD^{-1}$.

Заметим, что на втором шаге алгоритма расшифрования вычисляется вектор ошибок по синдромному вектору, а не по искаженному вектору.

Приведем также модификацию алгоритма расшифрования сообщения $y = e\widetilde{H}^T$.

1. Умножение полученного вектора y на $(C^T)^{-1}$:

$$S = y(C^T)^{-1} = eDP^TH^T = \widetilde{e}H^T,$$

где $\widetilde{e} = eDP^T$, $wt(\widetilde{e}) = wt(e)$.

2. Нахождение какого-либо вектора $\widetilde{x}$, который является решением относительно x уравнения $S = xH^T$ (т. е. $\widetilde{e}$ и $\widetilde{x}$ имеют одинаковые синдромы и поэтому принадлежат одному смежному классу, причем $u = \widetilde{x} - \widetilde{e}$ — кодовое слово, поэтому $\widetilde{x} = u + \widetilde{e}$. Следовательно, $\widetilde{x}$ является вектором вида $\widetilde{x} = iG + \widetilde{e}$ для некоторого неизвестного информационного вектора i).

3. Нахождение вектора ошибок $\widetilde{e}$ с помощью алгоритма декодирования, примененного для вектора $\widetilde{x}$.

4. Нахождение исходного сообщения e путем умножения вектора $\widetilde{e}$ на PD^{-1}: $e = \widetilde{e}PD^{-1}$.

Заметим, что $S = xH^T$ — синдромный вектор и что $\widetilde{e}$ является одним из решений уравнения $S = xH^T$ относительно x. Нахождение какого-либо решения этого уравнения является простой задачей, так как это система из $n-k$ линейных уравнений с n неизвестными. Но нахождение из всех решений вектора минимального веса является очень сложной задачей.

Если использовать коды Гоппы, то многочлен $G(x)$ может выступать дополнительным секретным параметром.

Теорема 1 ([12]). Пусть H — двоичная матрица размера $(n-k)\times n$, $S = eH^T$ — ненулевой синдромный вектор, $wt(e) \leqslant t$. Тогда нахождение двоичного вектора e веса не более t с синдромом S является NP-полной задачей.

В работе [13] показано, что стойкости криптосистем Мак-Элиса и Нидеррайтера эквивалентны, поэтому любую эффективную атаку на одну из схем можно легко преобразовать в атаку на другую схему.

Для криптосистемы Нидеррайтера также имеется модернизированный вариант (с использованием кодов $\Gamma(L,G)$) для уменьшения объема хранимой информации. Алгоритм выработки открытого ключа H для модернизированной криптосистемы имеет следующий вид.

1. Случайным образом генерируется многочлен $G(x)$ степени r над полем $GF(q^m)$ (например, можно сгенерировать неприводимый многочлен).
2. Случайным образом выбираются n элементов поля $GF(q^m)$, не являющиеся корнями многочлена $G(x)$, которые определяют множество L. Если $G(x)$ неприводим, то можно взять любые различные n элементов поля $GF(q^m)$.
3. Вычисляется проверочная матрица H' размера $r\times n$ на основе L и $G(x)$.
4. С помощью элементарных преобразований строк и перестановки столбцов матрица H' приводится к каноническому виду $H = CH'P = (Q^T_{(n-k)\times k},\, I_{n-k})$. L также умножается на P справа.
5. На основе матрицы H вычисляется порождающая матрица G в канонической форме: $G = (I_k,\, Q_{k\times(n-k)})$.

Шифрование сообщения в модернизированной криптосистеме совпадает с классической версией $y = eH^T$, разве что необходимо выполнить меньшее число операций. Для расшифрования сообщения необходимо выполнить следующие действия.

1. Вычисляется $S = y(C^T)^{-1} = eP^TH'^T = \widetilde{e}H'^T$, где $\widetilde{e} = eP^T$, $wt(\widetilde{e}) = wt(e)$.
2. С помощью алгоритма декодирования по синдромному вектору S находится вектор $\widetilde{e}$, после чего вычисляется $e = \widetilde{e}P$.

Пример 2 (классическая криптосистема Нидеррайтера). Рассмотрим, как и в примере 1, расширение $GF(2)\subset GF(2^4)$, $L = GF(2^4) = \{0,1,\alpha,\alpha^2,\ldots,\alpha^{14}\}$, многочлен $G(x) = x^2+x+\alpha^3$, код $\Gamma(L,G)$ с проверочной матрицей H. Матрицы C и P возьмем из примера 1.

Абонент A вычисляет матрицу:

$$\widetilde{H} = CHP = \begin{pmatrix} 0&0&1&0&0&0&1&0&1&0&1&1&0&0&1&0\\ 1&1&1&1&0&0&0&0&1&0&1&1&1&0&1&1\\ 0&0&0&0&0&0&1&1&1&0&0&0&1&0&1&1\\ 1&0&0&1&1&0&1&0&1&1&1&1&1&1&1&0\\ 1&0&1&0&1&0&0&1&1&0&1&1&1&0&1&0\\ 0&1&1&1&0&1&0&1&1&0&0&1&1&0&0&0\\ 0&1&1&1&0&1&0&0&0&1&0&1&1&1&0&1\\ 1&0&0&0&1&1&0&1&1&1&1&1&1&0&0&1 \end{pmatrix}.$$

Параметры n, k, t и матрица $\widetilde{H}$ являются открытым ключом абонента A.

Абонент B помещает сообщение x в вектор ошибок e длины n веса не более $t=2$. Пусть

$$e = (0,0,1,0,0,0,0,0,0,0,1,0,0,0,0,0).$$

Абонент B шифрует сообщение e с помощью открытого ключа $\widetilde{H}$:

$$y = e\widetilde{H} = (0,0,0,1,0,1,1,1).$$

Шифрованное сообщение y передается по открытому каналу связи абоненту A.

Абонент A, получив сообщение y, расшифровывает его следующим образом. Сначала происходит умножение вектора y на матрицу $(C^T)^{-1} = (C^{-1})^T$:

$$S = y(C^T)^{-1} = (1,1,0,1,0,1,1,0).$$

Зафиксируем частное решение $\widetilde{x}$ системы уравнений $xH^T = S$:

$$\widetilde{x} = (0,0,0,0,1,1,1,0,0,0,0,0,0,0,0,0).$$

После применения к вектору $\widetilde{x}$ алгоритма декодирования, например алгоритма Паттерсона:

$$S(x) \equiv \alpha^{13} + \alpha^7 x, \quad T(x) \equiv S^{-1}(x) \equiv \alpha^{14} + \alpha x,$$

$$p(x) \equiv \sqrt{T(x) + x} \equiv \alpha^8 + \alpha^2 x,$$

$$\sigma(x) = r_0^2(x) + x v_0^2(x) = \alpha + x + \alpha^4 x, \;\; X_1 = 1 = \alpha_1, \;\; X_2 = \alpha^{12} = \alpha_{13},$$

получаем вектор ошибок $\widetilde{e}$:

$$\widetilde{e} = (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0).$$

Для нахождения вектора e осталось вычислить:

$$e = \widetilde{e}P = (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0).$$

3. Современная кодовая криптосистема

Рассмотрим современную кодовую криптосистему [14; 15] на основе кодов Гоппы, которая использует идеи крипосистем Мак-Элиса и Нидеррайтера.

Генерация ключа. Абонент A производит следующую последовательность действий.

1. Генерация случайным образом неприводимого многочлена $G(x) \in GF(2^m)$ степени $r = t$.

2. Случайным образом выбирается множество $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ различных элементов поля $GF(2^m)$.

3. Вычисляется проверочная матрица H' размера $r \times n$ на основе множества L и многочлена $G(x)$: $(H')_{ij} = \alpha_j^{i-1} G(\alpha_j)^{-1}$.

4. Пусть $\beta_1, \ldots, \beta_m$ — базис пространства $GF(2^m)$ над $GF(2)$ (например, если α — примитивный элемент поля $GF(2^m)$, то можно взять $\beta_i = \alpha^{i-1}$, $i = 1, \ldots, m$). Каждый элемент матрицы H' заменяется двоичным вектором-столбцом длины m с компонентами из поля $GF(2)$, где данный столбец является координатным столбцом элемента матрицы H' в базисе $\beta_1, \ldots, \beta_m$. Тем самым получим двоичную матрицу $\widetilde{H}$ размера $rm \times n$ над $GF(2)$.

5. С помощью элементарных преобразований строк матрица $\widetilde{H}$ приводится к систематическому виду $H = (I_{n-k}, Q_{(n-k),k})$. Если это невозможно, то происходит переход в шаг 1.

После таких манипуляций открытым ключом абонента A являются n, k, t, $H = (I_{n-k}, Q)$. Секретным ключом являются параметры L и $G(x)$ неприводимого (следовательно, сепарабельного) кода Гоппы $\Gamma(L, G)$ длины n и размерности $k = n - mr$.

Шифрование сообщения. Пусть h — некоторая хеш-функция (например, с длиной свертки 256), e — двоичный открытый текст веса t. Алгоритм шифрования абонентом B сообщения e на основе открытого ключа абонента B имеет следующий вид.

1. Вычисление двоичного вектора $c_0 = eH^T = e(I_{n-k}, Q)^T$ длины mr.

2. Вычисление значения хеш-функции от e: $c_1 = h(e)$.

Шифрованным сообщением будет являться пара (c_0, c_1).

Расшифрование сообщения. После получения сообщения (c_0, c_1) для его расшифрования абонент A проделывает следующие шаги.

1. Вектор c_0 дополняется $k = n - rm$ нулями до длины n: $v = (c_0, 0, \ldots, 0)$.

2. С помощью алгоритма декодирования находится (единственный) кодовый вектор $u \in \Gamma(L, G)$, находящийся на расстоянии Хэмминга до вектора v не более t, т. е. $d(u, v) \leqslant t$ (ниже приводится этому обоснование).

3. Вычисляется вектор $\widetilde{e} = v - u$.

4. Если $wt(\widetilde{e}) = t$, $\widetilde{e}H^T = c_0$ и $h(\widetilde{e}) = c_1$, то $e = \widetilde{e}$ — исходный открытый текст.

Заметим, что на втором шаге алгоритма расшифрования синдром вектора v совпадает с c_0: $vH^T = c_0$. Действительно, $vH^T = v(I_{n-k}, Q_{(n-k),k})^T = v\begin{pmatrix} I_{n-k} \\ Q^T_{k,(n-k)} \end{pmatrix} = c_0$. Поэтому векторы e и v имеют одинаковые синдромы, значит, принадлежат одному смежному классу. Следовательно, искомый кодовый вектор равен $u = v - e$.

Замечание 2. Алгоритмы шифрования и расшифрования можно модернизировать следующим образом. Пусть x — исходный двоичный открытый текст, длина которого совпадает с длиной сверок хеш-функции h. Генерируется случайный двоичный вектор (ошибок) e длины n веса t, вычисляются $c_0 = eH^T$, $c_1 = h(e)$, $y = x \oplus c_1$. Шифрованным сообщением будет являться пара (c_0, y). Для расшифрования производятся следующие действия: $v = (c_0, 0, \ldots, 0)$, находится кодовый вектор $u \in \Gamma(L, G)$ со свойством $d(u, v) \leqslant t$, вычисляются $e = v - u$, $c_1 = h(e)$. Тогда $x = y \oplus c_1$.

4. Протоколы аутентификации на основе кодовых криптосистем

Построение протоколов аутентификации с нулевым разглашением можно реализовать, используя известные алгоритмы открытого шифрования. В качестве секретной информации, которой владеет доказывающая сторона A, будет использоваться секретный ключ x асимметричного шифра. Пусть D_x — алгоритм расшифрования на секретном ключе x, E_y — алгоритм шифрования на открытом ключе y. Проверяющая сторона шифрует некоторое сообщение M на открытом ключе y и передает криптограмму $C = E_y(M)$ абоненту A. Абонент A демонстрирует владение секретной информацией x тем, что расшифровывает сообщение своим секретным ключом: $M = D_x(C)$ и передает сообщение M проверяющей стороне B. Для проверяющей стороны B это не несет никакой дополнительной информации о секретном ключе x, так как у B до этого было то же самое сообщение M. При этом при построении протоколов с нулевым разглашением знания нужен некоторый механизм, который позволит владельцу секретного ключа (доказывающему A) до передачи восстановленного сообщения M проверяющему B убедиться в том, что последнее уже известно проверяющему B.

В качестве такого механизма могут использоваться алгоритмы хеширования (хеш-функции). Данный механизм используется в протоколах с нулевым разглашением, описанных в стандарте [16].

В стандарте [16] регламентируется формирование запроса в виде пары значений (C, H), где C — шифртекст, полученный путем шифрования некоторого сообщения M по открытому ключу доказывающего A, и H — значение хеш-функции, вычисленное от сообщения M с использованием некоторой хеш-функции h: $H = h(M)$. Получая запрос (C, H), доказывающий имеет возможность убедиться в том, что восстановленное им из шифртекста C сообщение M известно проверяющему. Для этого достаточно вычислить значение хеш-функции от восстановленного сообщения и сравнить его со значением второго элемента запроса.

В соответствии с [16] двухшаговый протокол с нулевым разглашением знания включает следующие шаги.

1. Проверяющий B выбирает произвольное сообщение M и, используя алгоритм открытого шифрования E_y и открытый ключ y доказывающего, зашифровывает сообщение M: $C = E_y(M)$. Затем, используя хеш-функцию h, вычисляет значение хеш-функции от : $H = h(M)$. После этого он отправляет доказывающему A пару значений (C, H) в качестве своего запроса.

2. Доказывающий A расшифровывает криптограмму C, используя свой личный секретный ключ x, в результате чего получает сообщение $\widetilde{M} = D_x(C)$. Затем он вычисляет значение хеш-функции от $\widetilde{M}$: $\widetilde{H} = h(\widetilde{M})$, сравнивает значения $\widetilde{H}$ и H, если $\widetilde{H} = H$, то отправляет проверяющему значение $\widetilde{M}$ в качестве своего ответа.

3. Если выполнено равенство $\widetilde{M} = M$, то проверяющий B принимает доказательство; если равенство не выполнено, то отвергает.

Протокол аутентификации на основе классической криптосистемы Мак-Элиса. Абонент A фиксирует порождающую матрицу G некоторого $[n, k, d]$-кода над $GF(q)$, исправляющего t и менее ошибок, невырожденную матрицу S порядка k над полем $GF(q)$, перестановочную и диагональную матрицы P и D порядка n.

Матрица $\widetilde{G} = SGPD$ является открытым ключом абонента A, как и параметры n, k, t. Маскирующие матрицы S, P, D и порождающая матрица G являются секретным ключом абонента A.

Протокол аутентификации имеет следующий вид.

1. Проверяющий B генерирует случайное сообщение M длины k с компонентами из $GF(q)$, а также вектор ошибок e длины n над $GF(q)$ веса не более t. Вычисляет $C = M\widetilde{G} + e$, $H = h(M)$ и отправляет доказывающему A пару значений (C, H).

2. Доказывающий A вычисляет $C' = CD^{-1}P^{-1}$, декодирует вектор M' на основе вектора C', вычисляет $\widetilde{M} = M'S^{-1}$, вычисляет $\widetilde{H} = h(\widetilde{M})$. Если $\widetilde{H} = H$, то отправляет проверяющему значение $\widetilde{M}$ в качестве своего ответа.

3. После этого проверяющий B проверяет равенство $\widetilde{M} = M$.

Аналогичным образом можно использовать любую кодовую криптосистему в качестве основы для протокола аутентификации.

Выводы

Рассмотренная в работе тема является актуальной, так как затрагивает вопрос существования постквантовых криптосистем с открытым ключом. Приведены некоторые вариации кодовых криптосистем, включая некоторые современные модификации на основе кодов Гоппы. Приводится пример декодирования кода Гоппы на основе алгоритма Паттерсона. Также в работе предложен вариант протокола аутентификации на основе кодовых криптосистем. Представленный протокол имеет нулевое разглашение знания.

Литература

[1] McEliece R.J. A Public-Key Cryptosystem Based On Algebraic Coding Theory // DSN Progress Report. 1978. Vol. 42–44. P. 114–116.

[2] Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. National Institute of Standards and Technology. Internal Report 8240. January, 2019. 27 p. DOI: http://doi.org/10.6028/NIST.IR.8240.

[3] Patterson N.J. The algebraic decoding of Goppa codes // IEEE Transactions on Information Theory. 1975. Vol. 21, №. 2. P. 203–207. DOI: https://doi.org/10.1109/TIT.1975.1055350.

[4] Рацеев С.М. Об алгоритмах декодирования кодов Гоппы // Челяб. физ.-матем. журн. 2020. Т. 5, № 3. С. 327–341. DOI: https://doi.org/10.47475/2500-0101-2020-15307.

[5] Рацеев С.М., Череватенко О.И. О простом алгоритме декодировании кодов БЧХ, кодов Рида — Соломона и кодов Гоппы // Вестник СибГУТИ. 2020. № 3 (51). С. 3–14. URL: https://www.elibrary.ru/item.asp?id=44408789; http://vestnik.sibsutis.ru/showpapper.php?act=showpapper&id=950

[6] Рацеев С.М., Череватенко О.И. Об алгоритмах декодирования обобщенных кодов Рида — Соломона // Системы и средства информатики. 2020. Т. 30, № 4. С. 83–94. DOI: https://doi.org/10.14357/08696527200408.

[7] Рацеев С.М., Череватенко О.И. Об алгоритмах декодирования обобщенных кодов Рида — Соломона на случай ошибок и стираний // Вестник Самарского университета. Естественнонаучная серия. 2020. Т. 26, № 3. С. 17–29. DOI: https://doi.org/10.18287/2541-7525-2020-26-3-17-29.

[8] Bhaskar Biswas, Nicolas Sendrier. McEliece Cryptosystem Implementation: Theory and Practice // Buchmann J., Ding J. (eds.) Post-Quantum Cryptography. PQCrypto 2008. Lecture Notes in Computer Science. Vol. 5299. Springer, Berlin; Heidelberg, 2008. DOI: https://doi.org/10.1007/978-3-540-88403-3_4.

[9] Fitzpatrick P., Ryan J.A. Counting irreducible Goppa codes. Conference: Workshop on Coding and Cryptography (WCC). Versaille, France. Volume: 2003. March, 2003. URL: https://www.researchgate.net/publication/276265397_Counting_irreducible_Goppa_codes.

[10] Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory // Problems of Control and Information Theory. 1986. Vol. 15, № 2. P. 159–166.

[11] Bernstein Daniel J., Buchmann Johannes, Dahmen Erik (eds.) Post-Quantum Cryptography. Berlin, Heidelberg: Springer-Verlag, 2009. DOI: http://dx.doi.org/10.1007/978-3-540-88702-7_4.

[12] Berlekamp E., McEliece R.J., Tilborg H. Van. On the inherent intractability of certain coding // IEEE Transactions on Information Theory. 1978. Vol. IT-24, № 3. P. 384–386. DOI: https://doi.org/10.1109/TIT.1978.1055873.

[13] Сидельников В.М. Криптография и теория кодирования // Московский университет и развитие криптографии в России: материалы конференции. Москва: МГУ, 2002. 22 с.

[14] Wang W., Szefer J., Niederhagen R. FPGA-based key generator for the niederreiter cryptosystem using binary Goppa codes. In: Fischer W., Homma N. (eds.) Cryptographic Hardware and Embedded Systems – CHES 2017 // CHES 2017. Lecture Notes in Computer Science. Vol. 10529. P. 253–274. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-66787-4_13.

[15] Bernstein D., Chou T., Lange T., Maurich I., Misoczki R., Niederhagen R., Persichetti E., Peters C., Schwabe P., Sendrier N., Szefer J., Wang W. Classic McEliece: conservative code-based cryptography. Project documentation. URL: https://classic.mceliece.org/nist/mceliece-20190331.pdf, свободный. Яз. англ. (дата обращения: 02.12.2020).

[16] ISO/IEC 9798-5:2009(E) «Information technology – Security techniques – Entity authentication – Part 5: Mechanisms using zero-knowledge technique». URL: https://www.iso.org/standard/50456.html.

Scientific article

DOI: 10.18287/2541-7525-2021-27-1-62-73

Submited: 11.12.2020
Revised: 20.01.2021
Accepted: 28.02.2021

S.M. Ratseev
Ulyanovsk State University, Ulyanovsk, Russian Federation
E-mail: ratseevsm@mail.ru. ORCID: https://orcid.org/0000-0003-4995-9418
O.I. Cherevatenko
Ulyanovsk State University of Education, Ulyanovsk, Russian Federation
E-mail: chai@pisem.net. ORCID: https://orcid.org/0000-0003-3931-9425
V.A. Chernyavskaya
Ulyanovsk State University, Ulyanovsk, Russian Federation
E-mail: vera.chernya@yandex.ru. ORCID: https://orcid.org/0000-0001-9875-2232

ON SOME CRYPTOSYSTEMS BASED ON ALGEBRAIC CODES

ABSTRACT

In 1978 McEliece built the first public key cryptosystem based on error-correcting codes. At the same time, effective attacks on the secret keys of this cryptosystem have not yet been found. The work describes the classical and modernized cryptosystems of McEliece and Niederreiter, also examples of their practical application based on Goppa codes using the Patterson algorithm. Also the algorithms of two-step authentication protocols with zero disclosure based on error-correcting codes are given.

Key words: McEliece cryptosystem; error-correcting codes; Goppa codes; code decoding.

Citation. Ratseev S.M., Cherevatenko O.I., Chernyavskaya V.A. On some cryptosystems based on algebraic codes. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2021, vol. 27, no. 1, pp. 62–73. DOI: http://doi.org/10.18287/2541-7525-2021-27-1-62-73. (In Russ.)

Information about the conflict of interests: authors and reviewers declare no conflict of interests.

© Ratseev S.M., 2021
Sergey Mihaylovich Ratseev — Doctor of Physical and Mathematical Sciences, associate professor, Department of Information Security and Control Theory, Ulyanovsk State University, 42, Leo Tolstoy Street, Ulyanovsk, 432017, Russian Federation.

© Cherevatenko O.I., 2021
Olga Ivanovna Cherevatenko — Candidate of Physical and Matheatical Sciences, associate professor, Department of Higher Mathematics, Ulyanovsk State University of Education, 4/5, Lenin Square, Ulyanovsk, 432063, Russian Federation.

© Chernyavskaya V.A., 2021
Vera Alekseevna Chernyavskaya — student of the Department of Information Security and Control Theory, Ulyanovsk State University, 42, Leo Tolstoy Street, Ulyanovsk, 432017, Russian Federation.

References

[1] McEliece R.J. A Public-Key Cryptosystem Based On Algebraic Coding Theory. *DSN Progress Report*, 1978, no. 42–44, pp. 114–116.

[2] Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. National Institute of Standards and Technology. Internal Report 8240. January, 2019, 27 p. DOI: https://doi.org/10.6028/NIST.IR.8240

[3] Patterson N.J. The algebraic decoding of Goppa codes. *IEEE Transactions on Information Theory*, 1975, vol. 21, no. 2, pp. 203–207. DOI: https://doi.org/10.1109/TIT.1975.1055350.

[4] Ratseev S.M. On decoding algorithms for Goppa codes. *Chelyabinskiy Fiziko-Matematicheskiy Zhurnal = Chelyabinsk Physical and Mathematical Journal*, 2020, vol. 5, no. 3, pp. 327–341. DOI: https://doi.org/10.47475/2500-0101-2020-15307. (In Russ.)

[5] Ratseev S.M., Cherevatenko O.I. On a simple algorithm for decoding BCH codes, Reed-Solomon codes, and Goppa codes. *Vestnik SibGUTI*, 2020, № 3 (51), pp. 3–14. Available at: https://www.elibrary.ru/item.asp?id=44408789; http://vestnik.sibsutis.ru/showpapper.php?act=showpapper&id=950. (In Russ.)

[6] Ratseev S.M., Cherevatenko O.I. On decoding algorithms for generalized Reed-Solomon codes. *Sistemy i Sredstva Informatiki* = Systems and Means of Informatics, 2020, vol. 30, issue 4, pp. 83–94. DOI: https://doi.org/10.14357/08696527200408. (In Russ.)

[7] Ratseev S.M., Cherevatenko O.I. On decoding algorithms for generalized Reed-Solomon codes with errors and erasures. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2020, vol. 26, no. 3, pp. 17–29. DOI: https://doi.org/10.18287/2541-7525-2020-26-3-17-29. (In Russ.)

[8] Bhaskar Biswas, Nicolas Sendrier. McEliece Cryptosystem Implementation: Theory and Practice. In: Buchmann J., Ding J. (eds.) *Post-Quantum Cryptography. PQCrypto 2008. Lecture Notes in Computer Science*, 2008, vol 5299, pp. 47–62. Springer, Berlin; Heidelberg. DOI: https://doi.org/10.1007/978-3-540-88403-3_4.

[9] Fitzpatrick P., Ryan J.A. Counting irreducible Goppa codes. *Workshop on Coding and Cryptography (WCC).* At: Versaille, France. Voleume: 2003. Available at: https://www.researchgate.net/publication/276265397_Counting_irreducible_Goppa_codes.

[10] Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 1986, vol. 15, no. 2, pp. 159–166.

[11] Bernstein Daniel J.; Buchmann Johannes; Dahmen Erik (eds.) Post-Quantum Cryptography. Berlin; Heidelberg: Springer-Verlag, 2009, pp. 95–145. DOI: http://dx.doi.org/10.1007/978-3-540-88702-7_4.

[12] Berlekamp E., McEliece R.J., Tilborg H. Van. On the inherent intractability of certain coding. *IEEE Transactions on Information Theory*, 1978, vol. IT-24, no. 3, May 1978, pp. 384–386. DOI: https://doi.org/10.1109/TIT.1978.1055873.

[13] Sidelnikov V.M. Cryptography and coding theory. In: *Materials of the conference «Moscow State University and Development of Cryptography in Russia»*. Moscow: MGU, 2002, 22 p. (In Russ.)

[14] Wang W., Szefer J., Niederhagen R. FPGA-based key generator for the niederreiter cryptosystem using binary Goppa codes. In: Fischer W., Homma N. (eds.) *Cryptographic Hardware and Embedded Systems – CHES 2017*. CHES 2017. Lecture Notes in Computer Science, 2017, vol. 10529, pp. 253–274. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-66787-4_13.

[15] Bernstein D., Chou T., Lange T., Maurich I., Misoczki R., Niederhagen R., Persichetti E., Peters C., Schwabe P., Sendrier N., Szefer J., Wang W. Classic McEliece: conservative code-based cryptography. Project documentation. Available at: https://classic.mceliece.org/nist/mceliece-20190331.pdf (accessed: 02.12.2020).

[16] ISO/IEC 9798-5:2009(E) Information technology – Security techniques – Entity authentication – Part 5: Mechanisms using zero-knowledge technique. Available at: https://www.iso.org/standard/50456.html.

Научная статья
DOI: 10.18287/2541-7525-2021-27-1-74-80

УДК 517+531.01

Дата: поступления статьи: 27.12.2020
после рецензирования: 18.01.2021
принятия статьи: 28.02.2021

М.В. Шамолин
Институт механики Московского государственного университета
имени М.В. Ломоносова, г. Москва, Российская Федерация
E-mail: shamolin@rambler.ru, shamolin@imec.msu.ru. ORCID: http://orcid.org/0000-0002-9534-0213

ЗАДАЧИ ДИФФЕРЕНЦИАЛЬНОЙ И ТОПОЛОГИЧЕСКОЙ ДИАГНОСТИКИ. ЧАСТЬ 6. СТАТИСТИЧЕСКОЕ РЕШЕНИЕ ЗАДАЧИ ДИФФЕРЕНЦИАЛЬНОЙ ДИАГНОСТИКИ[1]

АННОТАЦИЯ

Данная работа является шестой работой цикла по дифференциальной и топологической диагностике. В работе показано, что диагностика в случае траекторных измерений с шумом, представляющим собой случайный процесс типа нормального белого шума с нулевым средним значением и ограниченным спектром, осуществима с помощью алгоритмов диагностирования, полученных в предыдущих работах этого цикла, то есть результаты данной работы остаются справедливыми и в этом достаточно общем случае, при этом получен функционал диагностирования, который в предыдущих работах этого цикла вводился априори.

Ключевые слова: задача диагностирования; алгоритмы диагностирования; статистическое решение.

Цитирование. Шамолин М.В. Задачи дифференциальной и топологической диагностики. Часть 6. Статистическое решение задачи дифференциальной диагностики // Вестник Самарского университета. Естественнонаучная серия. 2021. Т. 27, № 1. С. 74–80. DOI: http://doi.org/10.18287/2541-7525-2021-27-1-74-80.

Информация о конфликте интересов: автор и рецензенты заявляют об отсутствии конфликта интересов.

© Шамолин М.В., 2021

Максим Владимирович Шамолин — доктор физико-математических наук, профессор, ведущий научный сотрудник Института механики, академик РАЕН, Московский государственный университет имени М.В. Ломоносова, 119192, Российская Федерация, г. Москва, Мичуринский пр., 1.

Введение

В предыдущей статье цикла [5] в рамках доказательства предельной теоремы была показана возможность диагностики динамических управляемых систем в случае траекторных измерений с ошибкой ограниченной по модулю заданной функцией времени и в случае, если эта ошибка является случайной величиной, распределенной по нормальному закону с дисперсией σ^2 [1–5]. Также было и будет показано, что в этих случаях можно указать «наилучшее» число необходимых траекторных измерений, при которых возможно разделение траекторий неисправных систем, то есть точное определение происшедшей в системе неисправности [6; 7].

Покажем теперь, что с помощью предложенных алгоритмов можно осуществить диагностику динамических управляемых систем в случае траекторных измерений с шумом, исходя из более общих вероятностных представлений [8–10].

[1]Работа выполнена при финансовой поддержке РФФИ (грант 19-01-00016).

1. Статистические алгоритмы и дифференциальные уравнения

Напомним, что конечному набору опорных невырожденных неисправностей

$$H = \|H_j\|_{j=1}^{l} \tag{1.1}$$

из класса возможных, введенного в предыдущих работах данного цикла [2; 3], поставим в соответствие набор обыкновенных дифференциальных уравнений

$$x' = f_j(x,t),\ j = 1,\dots,l. \tag{1.2}$$

Здесь $f_j(x,t)$ — известные вектор-функции, отличающиеся друг от друга той или иной неисправностью (1.1). Модели (1.2) будем называть *невырожденными*. Таким образом, на выбор правых частей уравнений (1.2) вводятся некоторые ограничения (см. также [11; 12]).

В соответствии с (1.2) рассмотрим (вообще говоря, несколько другие) уравнения

$$x' = \bar{f}_j(x,t),\ j = 1,\dots,l \tag{1.3}$$

(в дальнейшем черту опустим).

Предположим, что в момент $t = 0$ произошла j-я неисправность, то есть в правой части (1.3) присутствует одна из функций $f_j(x,t)$, причем это может быть любая $f_j\,(j = 1,\dots,l)$ *с равной вероятностью*.

Предположим, что доступен наблюдению следующий вектор:

$$z(t) = x(t) + \xi(t),$$

где $x(t)$ — вектор состояния системы, а $\xi(t)$ — случайный процесс типа нормального белого шума с нулевым средним значением и ограниченным спектром $W(\omega)$ следующего вида:

$$W(\omega) = \begin{cases} M_0, |\omega| \leqslant \Delta; \\ 0, |\omega| > \Delta. \end{cases} \tag{1.4}$$

Величина $\xi(t)$ является *ошибкой измерения вектора состояния системы* $x(t)$ (см. также [13–15]).

На основе анализа наблюдаемого суммарного сигнала $z(t)$ можно вычислить распределение $P_z(x)$ для всех возможных значений сигнала $x(t)$. Распределение $P_z(x)$ называют распределением обратных вероятностей [32], так как оно указывает на то, каковы вероятности тех или иных значений причины x, если известно вызванное этой причиной следствие z.

На основе анализа этого распределения принимается решение о том, каково было значение сигнала $x(t)$, то есть в нашем случае — каков был номер правой части системы (1.3), решением которой является вектор x. Будем обозначать решение системы (1.3) с правой частью $f_j(x,t)$ буквой x с индексом j.

Номер j может быть определен, например, на основе принципа *максимальной обратной вероятности*, то есть в качестве j принимается номер решения x_j, для которого вероятность $P_z(x_j)$ имеет наименьшее значение (см. также [16; 17]).

Вероятность $P_z(x)$ находится из классических соотношений

$$P(x,z) = P(x)P_x(z) = P(z)P_z(x),$$

где $P(x,z)$ — совместная вероятность двух случайных функций x и z, $P_x(z)$— условная вероятность z при заданном x, $P(z)$— безусловная вероятность z.

Тогда, заменяя $1/P(z)$ на постоянную K (так как нас интересует зависимость $P_z(x)$ при данном измеренном z), получим:

$$P_z(x) = KP(x)P_x(z).$$

Постоянная K определяется из условия нормировки

$$\int\limits_{A_x} P_z(x)dx = 1,$$

где A_x — область всех возможных значений x.

Величины

$$P(x) = P(x_j) = \frac{1}{l}$$

(где l — число возможных правых частей (1.3)) априорно известны. Требуется найти зависимость величины $P_x(z)$ от x при данном измеренном z (см. также [18–20]).

При данном векторе $x_j(t)$ вероятность реализации величины $z(t)$ равна вероятности реализации величины

$$\xi_j(t) = z(t) - x_j(t).$$

Считая величины $\xi_j(t)$ и $x_j(t)$ *статистически независимыми*, получим [32]:

$$P_x(z) = F(\xi_j) = \frac{1}{(2\pi M)^N} e^{-\frac{1}{M_0}\int\limits_{\tau_0}^{\tau} \xi_j^2(t)dt}.$$

Здесь $M_0 = M/2\Delta$ — единичная интенсивность шума (1.4), M — средняя интенсивность, $N = [\Delta(\tau - \tau_0)]$ (квадратные скобки в данном случае означают взятие целой части числа), где Δ — ширина спектра, $\tau - \tau_0$ — время определения номера j (время диагностирования).

Таким образом, справедливо представление

$$P_x(z) = \frac{1}{(2\pi M)^N} e^{-\frac{1}{M_0}\int\limits_{\tau_0}^{\tau} (z(t)-x_j(t))^2 dt}.$$

Тогда

$$P_z(x_j) = \frac{K}{l}\frac{1}{(2\pi M)^N} e^{-\frac{1}{M_0}\int\limits_{\tau_0}^{\tau} (z(t)-x_j(t))^2 dt}. \tag{1.5}$$

В силу того, что величины K и l постоянны, величина $(2\pi M)^N$ в (1.5) при конкретном значении $\xi(t)$ и заданной разности $\tau - \tau_0$ также постоянна. Нахождение же максимума обратной вероятности сводится к нахождению максимума величины

$$e^{-\frac{1}{M_0}\int\limits_{\tau_0}^{\tau} (z(t)-x_j(t))^2 dt},$$

или, что то же самое, к нахождению минимума следующей величины:

$$\int\limits_{\tau_0}^{\tau} (z(t) - x_j(t))^2 dt \tag{1.6}$$

(так как $M_0 = \mathrm{const}$ при фиксированных величинах M и Δ) [21–23].

2. Преобразование ключевой величины и функционал

Покажем, что величина (1.6) путем использования теоремы Котельникова о разложении случайной функции может быть сведена от интеграла к сумме.

Действительно, так как время диагностирования $\tau - \tau_0$ задано и характеристика шума $\xi(t)$ известна (в частности, известна ширина спектра Δ), то по теореме Котельникова существует число $N = [\Delta(\tau - \tau_0)]$ такое, что N значений

$$\xi_j(t_i),\ i = 1, \ldots, N,\ \ t_i = \frac{i}{\Delta},$$

являются *некоррелированными* (а при нашем предположении о нормальности белого шума и статистически независимыми) координатами процесса $\xi_j(t)$, и на конечном интервале времени (τ_0, τ) применимо разложение следующего вида:

$$\int\limits_{\tau_0}^{\tau} \xi_j^2(t)\, dt = \sum_{i=1}^{N} \xi_j^2(t_i). \tag{2.1}$$

Моменты времени t_i в (2.1) являются моментами измерений вектора $z(t)$ в процессе функционирования системы. Для тех же моментов времени t_i (в бортовом вычислителе по модели объекта) вычисляются все вектора состояний [24; 25]:

$$\overline{x_j},\ j = 1, \ldots, l.$$

Решающее правило определения номера j правой части (1.3) сформулируем теперь следующим образом.

На интервале времени (τ_0, τ) для всех возможных значений номеров j правой части (1.3) формируются следующие суммы:

$$S_j = \sum_{i=1}^{N} (z(t) - \overline{x_j}(t))^2. \tag{2.2}$$

Число j, для которого значение S_j минимально, указывает номер правой части (1.3), то есть номер случившейся в системе неисправности.

Заключение

Таким образом, в результате статистического решения задачи дифференциальной диагностики при траекторных измерениях с шумом получен алгоритм диагностики, аналогичный алгоритму, который влечет теорема предыдущей работы цикла [5], а также функционал диагностики (2.2), который в теореме вводился априори, то есть получено *замкнутое детерминированное решение* задачи дифференциальной диагностики: получен функционал, решающий задачу, и указано правило его минимизации (см. также [26–28]).

Полученный алгоритм верен и в случае, если вектор $z(t)$ содержит несущее информацию о характере функций $f_j(x,t)$, $j = 1, \ldots, l$ в правых частях уравнений (1.3) подмножество $d < n$ измеряемых координат фазового вектора состояния $x(t)$ (ср. с [29; 30]).

Если динамическая управляемая система подвержена внутренним и внешним воздействиям шумов и математическая модель движения этой системы так или иначе описывает эти шумы, то диагностика управления такой системой также может быть осуществлена с помощью полученного алгоритма (см. также [31; 32]).

В дальнейшей работе данного цикла перейдем к конкретным задачам, касающимся систем прямого и непрямого управления.

Работа выполнена при финансовой поддержке РФФИ (грант 19-01-00016).

Литература

[1] Шамолин М.В. Задачи дифференциальной и топологической диагностики. Часть 1. Уравнения движения и классификация неисправностей // Вестник Самарского университета. Естественнонаучная серия. 2019. Т. 25, № 1. С. 32–43. DOI: https://doi.org/10.18287/2541-7525-2019-25-1-32-43.

[2] Шамолин М.В. Задачи дифференциальной и топологической диагностики. Часть 2. Задача дифференциальной диагностики // Вестник Самарского университета. Естественнонаучная серия. 2019. Т. 25, № 3. С. 22–31. DOI: https://doi.org/10.18287/2541-7525-2019-25-3-22-32.

[3] Шамолин М.В. Задачи дифференциальной и топологической диагностики. Часть 3. Задача контроля // Вестник Самарского университета. Естественнонаучная серия. 2019. Т. 25, № 4. С. 36–47. DOI: https://doi.org/10.18287/2541-7525-2019-25-4-36-47.

[4] Шамолин М.В. Задачи дифференциальной и топологической диагностики. Часть 4. Задача диагностирования (случай точных траекторных измерений) // Вестник Самарского университета. Естественнонаучная серия. 2020. Т. 26, № 1. С. 52–68. DOI: https://doi.org/10.18287/2541-7525-2020-26-1-52-68.

[5] Шамолин М.В. Задачи дифференциальной и топологической диагностики. Часть 5. Задача диагностирования (случай траекторных измерений с ошибкой) // Вестник Самарского университета. Естественнонаучная серия. 2020. Т. 26, № 3. С. 30–39. DOI: http://doi.org/10.18287/2541-7525-2020-26-3-30-39.

[6] Борисенок И.Т., Шамолин М.В. Решение задачи дифференциальной диагностики // Фундамент. и прикл. матем. 1999. Т. 5, Вып. 3. С. 775–790. DOI: http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=fpm&paperid=401&option_lang=rus.

[7] Шамолин М.В. Некоторые задачи дифференциальной и топологической диагностики. Изд. 2-е, перераб. и дополн. Москва: Экзамен, 2007. URL: http://eqworld.ipmnet.ru/ru/library/books/Shamolin2007-2ru.pdf.

[8] Shamolin M.V. Foundations of Differential and Topological Diagnostics // J. Math. Sci. 2003. Vol. 114, № 1. P. 976–1024. DOI: http://dx.doi.org/10.1023/A:1021807110899.

[9] Пархоменко П.П., Сагомонян Е.С. Основы технической диагностики. Москва: Энергия, 1981. URL: https://djvu.online/file/FmH1gaq0Jm2AJ.

[10] Мироновский Л.А. Функциональное диагностирование динамических систем // Автоматика и телемеханика. 1980. № 8. С. 96–121. URL: http://mi.mathnet.ru/at7158

[11] Окунев Ю.М., Парусников Н.А. Структурные и алгоритмические аспекты моделирования для задач управления. Москва: Изд-во МГУ, 1983.

[12] Чикин М.Г. Системы с фазовыми ограничениями // Автоматика и телемеханика. 1987. № 10. С. 38–46. URL: http://mi.mathnet.ru/at4566.

[13] Жуков В.П. О достаточных и необходимых условиях асимптотической устойчивости нелинейных динамических систем // Автоматика и телемеханика. 1994. № 3. С. 24–36. URL: http://mi.mathnet.ru/at3855

[14] Жуков В.П. О достаточных и необходимых условиях грубости нелинейных динамических систем в смысле сохранения характера устойчивости // Автоматика и телемеханика. 2008. № 1. С. 30–38. URL: http://mi.mathnet.ru/at587.

[15] Жуков В.П. О редукции задачи исследования нелинейных динамических систем на устойчивость вторым методом Ляпунова // Автоматика и телемеханика. 2005. № 12. С. 51–64. URL: http://mi.mathnet.ru/at1475.

[16] Борисенок И.Т., Шамолин М.В. Решение задачи дифференциальной диагностики методом статистических испытаний // Вестник МГУ. Сер. 1. Математика. Механика. 2001. № 1. С. 29–31. DOI: http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=vmumm&paperid=1441&option_lang=rus.

[17] Beck A., Teboulle M. Mirror Descent and Nonlinear Projected Subgradient Methods for Convex Optimization // Operations Research Letters. May 2003. Vol. 31, № 3. P. 167–175. DOI: https://doi.org/10.1016/S0167-6377(02)00231-6.

[18] Ben-Tal A., Margalit T., Nemirovski A. The Ordered Subsets Mirror Descent Optimization Method with Applications to Tomography // SIAM Journal on Optimization. 2001. Vol. 12, № 1. P. 79–108. DOI: https://doi.org/10.1137/S1052623499354564.

[19] Su W., Boyd S., Candes E. A Differential Equation for Modeling Nesterov's Accelerated Gradient Method: Theory and Insights // The Journal of Machine Learning Research. 2016. № 17 (153). P. 1–43. Available at: https://www.researchgate.net/publication/311221666_A_differential_equation_for_modeling_Nesterov's_accelerated_gradient_method_Theory_and_insights

[20] Шамолин М.В. Диагностика гиростабилизированной платформы, включенной в систему управления движением летательного аппарата // Электронное моделирование. 2011. Т. 33:3. С. 121–126. URL: http://dspace.nbuv.gov.ua/handle/123456789/61768.

[21] Шамолин М.В. Диагностика движения летательного аппарата в режиме планирующего спуска // Электронное моделирование. 2010. Т. 32:5. С. 31–44. URL: http://dspace.nbuv.gov.ua/handle/123456789/61677.

[22] Fleming W.H. Optimal Control of Partially Observable Diffusions // SIAM Journal on Control. 1968. Vol. 6, № 2. P. 194–214. DOI: https://doi.org/10.1137/0306015.

[23] Choi D.H., Kim S.H., Sung D.K. Energy-efficient Maneuvering and Communication of a Single UAV-based Relay // IEEE Transactions on Aerospace and Electronic Systems. 2014. Vol. 50, № 3. P. 2119–2326. DOI: https://doi.org/10.1109/TAES.2013.130074.

[24] Ho D.-T., Grotli E.I., Sujit P.B., Johansen T.A., Sousa J.B. Optimization of Wireless Sensor Network and UAV Data Acquisition // Journal of Intelligent & Robotic Systems. 2015. Vol. 78, № 1. P. 159–179. DOI: https://doi.org/10.1007/s10846-015-0175-5.

[25] Ceci C., Gerardi A., Tardelli P. Existence of Optimal Controls for Partially Observed Jump Processes // Acta Applicandae Mathematicae. 2002. Vol. 74, № 2. P. 155–175. DOI: http://dx.doi.org/10.1023/A:1020669212384.

[26] Rieder U., Winter J. Optimal Control of Markovian Jump Processes with Partial Information and Applications to a Parallel Queueing Model // Mathematical Methods of Operations Research. 2009. Vol. 70, № 3, P. 567–596. DOI: http://dx.doi.org/10.1007/s00186-009-0284-7.

[27] Power Control in Wireless Cellular Networks / M. Chiang [et al.] // Foundations and Trends in Networking. 2008. Vol. 2, № 4. P. 381–533. DOI: http://dx.doi.org/10.1561/1300000009.

[28] Power control in wireless cellular networks / E. Altman [et al.] // IEEE Transactions on Automatic Control. 2009. Vol. 54, № 10. P. 2328–2340. DOI: http://dx.doi.org/10.1109/tac.2009.2028960.

[29] Ober R.J. Balanced Parameterization of Classes of Linear Systems // SIAM Journal on Control and Optimization. 1991. Vol. 29, № 6. P. 1251–1287. DOI: https://doi.org/10.1137/0329065.

[30] Ober R.J., McFarlane D. Balanced Canonical Forms for Minimal Systems: A normalized Coprime Factor Approach // Linear Algebra and Its Applications. 1989. Vol. 122–124. P. 23–64. DOI: http://dx.doi.org/10.1016/0024-3795(89)90646-0.

[31] Antoulas A.C., Sorensen D.C., Zhou Y. On the Decay Rate of Hankel Singular Values and Related Issues // Systems & Control Letters. 2002. Vol. 46, № 5, P. 323–342. DOI: http://dx.doi.org/10.1016/S0167-6911(02)00147-0.

[32] Wilson D.A. The Hankel Operator and its Induced Norms // Int. J. Contr. 1985. Vol. 42. P. 65–70. DOI: https://doi.org/10.1080/00207178508933346.

Scientific article

DOI: 10.18287/2541-7525-2021-27-1-74-80

Submited: 27.12.2020
Revised: 18.01.2021
Accepted: 28.02.2021

M.V. Shamolin
Institute of Mechanics, Lomonosov Moscow State University, Moscow, Russian Federation
E-mail: shamolin@rambler.ru, shamolin@imec.msu.ru. ORCID: http://orcid.org/0000-0002-9534-0213

PROBLEMS OF DIFFERENTIAL AND TOPOLOGICAL DIAGNOSTICS. PART 6. STATISTICAL SOLVING OF THE PROBLEM OF DIFFERENTIAL DIAGNOSTICS[2]

ABSTRACT

Proposed work is the sixth work of the cycle on differential and topological diagnostics. It is shown that the diagnostics in the case of trajectorial measurements corrupted by noise, which is a stochastic process of the normal white noise type with zero mean value and bounded spectrum, can be performed by using the diagnostic algorithms obtained in [5], i.e., the results of this section remain valid even in this rather general case; moreover, the diagnostic functional, which was introduced in the theorem of [5] a priori, is now obtained a posteriori.

Key words: the diagnostic problem; diagnostic algorithms; statistical solving.

Citation. Shamolin M.V. Problems of differential and topological diagnostics. Part 6. Statistical solving of the problem of differential diagnostics. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2021, vol. 27, no. 1, pp. 74–80. DOI: http://doi.org/10.18287/2541-7525-2021-27-1-74-80. (In Russ.)

Information about the conflict of interests: author and reviewers declare no conflict of interests.

© Shamolin M.V., 2021

Maxim Vladimirovich Shamolin — Doctor of Physical and Mathematical Sciences, professor, leading researcher of the Institute of Mechanics, academic of the Russian Academy of Natural Sciences, Lomonosov Moscow State University, 1, Michurinsky Avenue, Moscow, 119192, Russian Federation.

References

[1] Shamolin M.V. Problems of differential and topological diagnostics. Part 1. Motion equations and classification of malfunctions. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2019, vol. 25, no. 1, pp. 32–43. Available at: https://doi.org/10.18287/2541-7525-2019-25-1-32-43. (In Russ.)

[2] Shamolin M.V. Problems of differential and topological diagnostics. Part 2. Problem of differential diagnostics. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2019, vol. 25, no. 3, pp. 22–31. DOI: https://doi.org/10.18287/2541-7525-2019-25-3-22-32. (In Russ.)

[3] Shamolin M.V. Problems of differential and topological diagnostics. Part 3. The checking problem. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2019, vol. 25, no. 4, pp. 36–47. DOI: https://doi.org/10.18287/2541-7525-2019-25-4-36-47. (In Russ.)

[4] Shamolin M.V. Problems of differential and topological diagnostics. Part 4. The case of exact trajectorial measurements. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2020, vol. 26, no. 1, pp. 52–68. DOI: https://doi.org/10.18287/2541-7525-2020-26-1-52-68.

[5] Shamolin M.V. Problems of differential and topological diagnostics. Part 5. The case of trajectorial measurements with error. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2020, vol. 26, no. 3, pp. 30–39. DOI: http://doi.org/10.18287/2541-7525-2020-26-3-30-39. (In Russ.)

[6] Borisenok I.T., Shamolin M.V. Solution of a problem of differential diagnostics. *Fundamental and Applied Mathematics*, 1999, vol. 5, no. 3, pp. 775–790. Available at: http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=fpm&paperid=401&option_lang=rus. (In Russ.)

[7] Shamolin M.V. Certain problems of differential and topological diagnostics. 2nd edition, revised and enlarged. Moscow: Ekzamen, 2007. Available at: http://eqworld.ipmnet.ru/ru/library/books/Shamolin2007-2ru.pdf. (In Russ.)

[8] Shamolin M.V. Foundations of Differential and Topological Diagnostics. *Journal of Mathematical Sciences*, 2003, vol. 114, no. 1, pp. 976–1024. DOI: http://dx.doi.org/10.1023/A:1021807110899.

[9] Parkhomenko P.P., Sagomonian E.S. Foundations of technical diagnostics. Moscow: Energiya, 1981. Available at: https://djvu.online/file/FmH1gaq0Jm2AJ. (In Russ.)

[10] Mironovskii L.A. Functional diagnosis of dynamic systems. *Avtomatika i Telemekhanika = Automation and Remote Control*, 1980, no. 8, pp. 96–121. Available at: http://mi.mathnet.ru/at7158. (In Russ.)

[2]The work is carried out with the financial support from Russian Foundation for Basic Research (grant 19-01-00016).

[11] Okunev Yu.M., Parusnikov N.A. Structural and Algorithmic Aspects of Modeling for Control Problems. Moscow: Izd-vo MGU, 1983. (In Russ.)

[12] Chikin M.G. Phase-constrained systems. *Avtomatika i Telemekhanika = Automation and Remote Control*, 1987, no. 10, pp. 38–46. Available at: http://mi.mathnet.ru/at4566. (In Russ.)

[13] Zhukov V.P. Sufficient and necessary conditions for the asymptotic stability of nonlinear dynamical systems. *Avtomatika i Telemekhanika = Automation and Remote Control*, 1994, vol. 55, no. 3, pp. 321–330. Available at: http://mi.mathnet.ru/at3855 (English; Russian original).

[14] Zhukov V.P. On the sufficient and necessary conditions for robustness of the nonlinear dynamic systems in terms of stability retention. *Avtomatika i Telemekhanika = Automation and Remote Control*, 2008, vol. 69, no. 1, pp. 27–35. DOI: https://doi.org/10.1134/S0005117908010037. (English; Russian original).

[15] Zhukov V.P. Reduction of Stability Study of Nonlinear Dynamic Systems by the Second Lyapunov Method. *Avtomatika i Telemekhanika = Automation and Remote Control*, 2005, vol. 66, no. 12, pp. 1916–1928. DOI: https://doi.org/10.1007/s10513-005-0224-9 (English; Russian original).

[16] Borisenok I.T., Shamolin M.V. Solving the problem of differential diagnostics by the method of statistical tests. *Vestnik Moskovskogo Universiteta. Seriya 1. Matematika. Mekhanika = Moscow University Mechanics Bulletin*, 2001, no. 1, pp. 29–31. Available at: http://mi.mathnet.ru/vmumm1441. (In Russ.)

[17] Beck A., Teboulle M. Mirror descent and nonlinear projected subgradient methods for convex optimization. *Operations Research Letters*, May 2003, vol. 31, Issue 3, pp. 167–175. DOI: https://doi.org/10.1016/S0167-6377(02)00231-6.

[18] Ben-Tal A., Margalit T., Nemirovski A. The Ordered Subsets Mirror Descent Optimization Method with Applications to Tomography. *SIAM Journal on Optimization*, 2001, vol. 12, no. 1, pp. 79–108. DOI: https://doi.org/10.1137/S1052623499354564.

[19] Su W., Boyd S., Candes E. A Differential Equation for Modeling Nesterov's Accelerated Gradient Method: Theory and Insights. *Journal of Machine Learning Research*, 2016, No. 17(153), pp. 1–43. Available at: https://www.researchgate.net/publication/311221666_A_differential_equation_for_modeling_Nesterov's_accelerated_gradient_method_Theory_and_insights.

[20] Shamolin M.V. Diagnostics of Gyro-Stabilized Platform, Included in the Aircraft Motion Control System. *Elektronnoe modelirovanie = Electronic Modeling*, 2011, vol. 33, no. 3, pp. 121–126. Available at: http://dspace.nbuv.gov.ua/handle/123456789/61768. (In Russ.)

[21] Shamolin M.V. Diagnostics of Aircraft Motion in Planning Descent Mode. *Elektronnoe modelirovanie = Electronic Modeling*, 2010, vol. 32, no. 5, pp. 31–44. Available at: http://dspace.nbuv.gov.ua/handle/123456789/61677. (In Russ.)

[22] Fleming W.H. Optimal Control of Partially Observable Diffusions. *SIAM Journal on Control*, 1968, vol. 6, no. 2, pp. 194–214. DOI: https://doi.org/10.1137/0306015.

[23] Choi D.H., Kim S.H., Sung D.K. Energy-efficient maneuvering and communication of a single UAV-based relay. *IEEE Transactions on Aerospace and Electronic Systems*, 2014, vol. 50, no. 3, pp. 2119–2326. DOI: https://doi.org/10.1109/TAES.2013.130074.

[24] Ho D.-T., Grotli E.I., Sujit P.B., Johansen T.A., Sousa J.B. Optimization of Wireless Sensor Network and UAV Data Acquisition. *Journal of Intelligent & Robotic Systems*, 2015, vol. 78, no. 1, pp. 159–179. DOI: https://doi.org/10.1007/s10846-015-0175-5.

[25] Ceci C., Gerardi A., Tardelli P. Existence of Optimal Controls for Partially Observed Jump Processes. *Acta Applicandae Mathematicae*, 2002, vol. 74, no. 2, pp. 155–175. DOI: http://dx.doi.org/10.1023/A:1020669212384.

[26] Rieder U., Winter J. Optimal Control of Markovian Jump Processes with Partial Information and Applications to a Parallel Queueing Model. *Mathematical Methods of Operations Research*, 2009, vol. 70, no. 3, pp. 567–596. DOI: http://dx.doi.org/10.1007/s00186-009-0284-7.

[27] Chiang M., Tan C.W., Hande P., Lan T. Power Control in Wireless Cellular Networks. *Foundations and Trends in Networking*, 2008, vol. 2, no. 4, pp. 381–533. DOI: http://dx.doi.org/10.1561/1300000009.

[28] Altman E., Avrachenkov K., Menache I., Miller G., Prabhu B.J., Shwartz A. Power control in wireless cellular networks. *IEEE Transactions on Automatic Control*, 2009, vol. 54, no. 10, pp. 2328–2340. Avaiilable at: http://dx.doi.org/10.1109/tac.2009.2028960.

[29] Ober R.J. Balanced Parameterization of Classes of Linear Systems. *SIAM Journal on Control and Optimization*, 1991, vol. 29, no. 6, pp. 1251–1287. DOI: https://doi.org/10.1137/0329065.

[30] Ober R.J., McFarlane D. Balanced canonical forms for minimal systems: a normalized coprime factor approach. *Linear Algebra and Its Applications*, 1989, vol. 122-124, pp. 23–64. DOI: http://dx.doi.org/10.1016/0024-3795(89)90646-0.

[31] Antoulas A.C., Sorensen D.C., Zhou Y. On the decay rate of Hankel singular values and related issues. *Systems & Control Letters*, 2002, vol. 46, no. 5, pp. 323–342. DOI: http://dx.doi.org/10.1016/S0167-6911(02)00147-0.

[32] Wilson D.A. The Hankel Operator and its Induced Norms. *International Journal of Control*, 1985, vol. 42, pp. 65–70. DOI: https://doi.org/10.1080/00207178508933346.

МЕХАНИКА
MECHANICS

Scientific article

DOI: 10.18287/2541-7525-2021-27-1-81-103

Submited: 11.01.2021
Revised: 15.02.2021
Accepted: 28.02.2021

S.A. Lychev
Ishlinsky Institute for Problems in Mechanics,
Russian Academy of Sciences, Moscow, Russian Federation
E-mail: lychevsa@mail.ru. ORCID: https://orcid.org/0000-0001-7590-1389
K.G. Koifman
Bauman Moscow State Technical University,
Moscow, Russian Federation
E-mail: koifman.konstantin@gmail.com. ORCID: https://orcid.org/0000-0002-7891-9995
A.V. Digilov
Ishlinsky Institute for Problems in Mechanics,
Russian Academy of Sciences, Moscow, Russian Federation
E-mail: avdigilov@gmail.com. ORCID: https://orcid.org/0000-0001-6892-7740

NONLINEAR DYNAMIC EQUATIONS FOR ELASTIC MICROMORPHIC SOLIDS AND SHELLS. PART I[1]

ABSTRACT

The present paper develops a general approach to deriving nonlinear equations of motion for solids whose material points possess additional degrees of freedom. The essential characteristic of this approach is the account of incompatible deformations that may occur in the body due to distributed defects or in the result of the some kind of process like growth or remodelling. The mathematical formalism is based on least action principle and Noether symmetries. The peculiarity of such formalism is in formal description of reference shape of the body, which in the case of incompatible deformations has to be regarded either as a continual family of shapes or some shape embedded into non-Euclidean space. Although the general approach yields equations for Cosserat-type solids, micromorphic bodies and shells, the latter differ significantly in the formal description of enhanced geometric structures upon which the action integral has to be defined. Detailed discussion of this disparity is given.

Key words: nonlinear dynamics; micropolar and micromorphic solids; shells; finite deformations; incompatibility of deformations; non-Euclidean reference shape; fiber bundles; enhanced material and physical manifolds; least action; Noether symmetries; field equations; conservation laws.

Citation. Lychev S.A., Koifman K.G., Digilov A.V. Nonlinear dynamic equations for elastic micromorphic solids and shells. Part I *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2021, vol. 27, no. 1, pp. 81–103. DOI: http://doi.org/10.18287/2541-7525-2021-27-1-81-103. (In Russ.)

Information about the conflict of interests: authors and reviewers declare no conflict of interests.

© Lychev S.A., 2021
Sergey Aleksandrovich Lychev — Doctor of Physical and Mathematical Sciences, leading researcher, Ishlinsky Institute for Problems in Mechanics, Russian Academy of Sciences, 101, Vernadsky Avenue, bldg. 1, Moscow, 119526, Russian Federation.

© Koifman K.G., 2021
Konstantin Georgievich Koifman — teaching assistant, Bauman Moscow State Technical University, 5, 2-nd Baumanskaya Street, Moscow, 105005, Russian Federation.

[1]The study was partially supported by the Government program (contract #AAAA-A20-120011690132-4) and partially supported by RFBR (grant No. 18-29-03228).

© Digilov A.V., 2021
Alexander Vyacheslavovich Digilov — postgraduate student, Ishlinsky Institute for Problems in Mechanics, Russian Academy of Sciences, 101, Vernadsky Avenue, bldg. 1, Moscow, 119526, Russian Federation.

Introduction

There is a widespread tendency at present to derive dynamic equations for shell-like solids by direct approach. In doing so, shells are regarded as two-dimensional Cosserat continuum, which additional degrees of freedom are associated with specific shell kinematics. From this point of view, models are similar to three-dimensional micromorphic solids and can be considered within a single mathematical formalism. However the geometric structure of the manifold representing the body has fundamentally different properties, depending on which model is considered. In the language of modern differential geometry, these differences are characterised by a particular bundle structure defined over a manifold that formalizes the shape of the body or its material counterpart. In this paper we have sought to answer on the question: how does the formal structure of bundle relate to the commonly accepted hypotheses in micropolar, micromorphic and shell-like bodies.

Mathematical shell theory is conventional field of continuum mechanics so it is unlikely that a complete literary list can be given here. We will give only some references [1–4]. The mathematical formalization of shell theory in Cosserat framework is also the subject of quite a lot of literature [5–8]. Non-linear models of shells whose deformations do not satisfy the compatibility conditions are much less developed. The works [9; 10] are the first such that should be mentioned here. In them, non-linear models are introduced within a general theory of materially inhomogeneous bodies, primarily developed by Truesdell and Noll in the framework of the material connection theory [11]. This approach has been developed in [12–14]. A slightly different approach based on the modeling of maps between manifolds with dimensions greater than 3 is represented in [15; 16]. Formally, this approach retains the idea of a geometric description for measures of deformation incompatibility in terms of material metric and connection, but defines them in high-dimensional spaces, which correspond to a set of material points, each of which has a continuous set of orientations. Models of this type have specific physical meaning, but it is very different from what is usually found in classical shell models. The latter can be obtained by considering the sections of bundles that form high-dimensional spaces. This issue is discussed in detail in present work.

1. Physical Space and Time

1°. Euclidean physical space and time. Generally, the geometrical approach developed in the paper, regards the body and the physical space as smooth manifolds of the common structure. However, with the application of the developed theory, we will confine ourselves to the specific case of a physical space with Euclidean structure and absolute time, as it is required by classical (non-relativistic) approach. Meanwhile, for the body, as the set of material points, we leave the possibility of being a smooth manifold of a general kind, because the difference between its geometry and Euclidean geometry is precisely that which characterizes the incompatible deformations.

We suppose that physical space can be formalized as three-dimensional Euclidean point space, which can be formulated as the structure[2]

$$\mathbb{E} = (E,\ \mathbb{V},\ \mathrm{vec},\ \cdot,\ \mathrm{or}). \tag{1.1}$$

The first element of the structure represents the underlying set E. Second element of (1.1) is three-dimensional real vector space $\mathbb{V} = (V,\ +_V,\ \cdot_V)$, in which V is the underlying set of translation vectors, $+_V : V \times V \to V$ is operation of addition, and $\cdot_V : \mathbb{R} \times V \to V$ is operation of multiplication on scalars. Points, i. e., elements of E, and translation vectors, i. e., elements of V, are related via the map

$$\mathrm{vec}:\ E \times E \to V, \quad (a,\ b) \mapsto \overrightarrow{ab} := \mathrm{vec}(a,\ b),$$

which belongs to the structure (1.1). The following Weyl axioms are satisfied [17]:

(a) for all three points $a,\ b,\ c \in E$ the Chasles' relation holds:

$$\overrightarrow{ab} + \overrightarrow{bc} = \overrightarrow{ac}.$$

[2]One and the same set X can be endowed with various structures, commonly represented by ordered lists of sets and mappings, that turn it into certain mathematical object. Algebraic, topological, smooth and geometric structures may serve as example. If Struct_1 and Struct_2 are structures on the set X then to distinguish between objects, defined by them, we denote these objects as tuples (X, Struct_1) and (X, Struct_2). For example, topology $\mathcal{T}$ and binary operation $\top$ on X define two structures: topological, $(X,\ \mathcal{T})$, and algebraic, $(X,\ \top)$.

(b) for arbitrary point $a \in E$ and arbitrary vector $\mathbf{v} \in V$ there exists a unique point $b \in E$, such that $\overrightarrow{ab} = \mathbf{v}$.

The symbol $(\cdot)$ from (1.1) stands for inner product[3] $\cdot : V \times V \to \mathbb{R}$ on $\mathbb{V}$, which is bilinear, symmetric and positive-definite functional. Finally, or is the chosen orientation of vector space $\mathbb{V}$, i. e., class $[(\boldsymbol{e}_i)_{i=1}^3]$ of bases under the following equivalence relation: bases $(\boldsymbol{e}_i)_{i=1}^3$ and $(\boldsymbol{e}'_i)_{i=1}^3$, $\boldsymbol{e}'_i = \Omega^j{}_i \boldsymbol{e}_i$, are similarly oriented if $\det[\Omega^i{}_j] > 0$. Here $[\Omega^i{}_j]$ is the transition matrix from basis $(\boldsymbol{e}_i)_{i=1}^3$ to basis $(\boldsymbol{e}'_i)_{i=1}^3$. By choosing an orientation, we restrict the set of acceptable bases to the corresponding class.

Having reference standards $(\boldsymbol{i}_k)_{k=1}^3$, one can construct reference standards for area and volume, which are represented by 2-vectors $\boldsymbol{i}_k \wedge \boldsymbol{i}_l$, i. e., oriented unit squares, and 3-vector $\boldsymbol{i}_1 \wedge \boldsymbol{i}_2 \wedge \boldsymbol{i}_3$, i. e., oriented unit cube. Moreover, the choice of inner product and orientation imply isomorphism $* : \mathbb{V} \wedge \mathbb{V} \to \mathbb{V}$, the Hodge star [17,18], from vector space of 2-vectors to vector space $\mathbb{V}$. This allows to introduce cross-product operation

$$[\cdot,\, \cdot] : \mathbb{V} \times \mathbb{V} \to \mathbb{V}, \quad [\boldsymbol{u},\, \boldsymbol{v}] := *(\boldsymbol{u} \wedge \boldsymbol{v}).$$

The absolute time is formalized as one-dimensional manifold $\mathbb{T}$, called chronometric. Its elements are instants of time. Appealing to daily observations, we suppose that $\mathbb{T}$ can be ordered, from "past" to "future". Besides spatial reference standards one has another, temporal reference standard. It defines coordinatization $\mathbb{T} \to \mathbb{R}$ of chronometric manifold $\mathbb{T}$. Assuming that reference standard is fixed, we identify chronometric manifold with real line $\mathbb{R}$.

2°. Enhanced physical space. The above mathematical formalization of the physical space $\mathbb{E}$ contains points which have conventional degrees of freedom only. To describe solids with extra degrees of freedom one needs to enhance the structure of $\mathbb{E}$. Possible way is to associate some m-dimensional manifold $\mathbb{F}$ with each point of $\mathbb{E}$. To formalize this structure in terms of smooth manifolds, further simple reasoning is needed. One can define $(3+m)$-dimensional product manifold $\mathbb{E} \times \mathbb{F}$. The submanifold $\{x\} \times \mathbb{F}$, which is topologically equivalent to $\mathbb{F}$, serves as manifold of possible extra spatial degrees of freedom associated with place $x \in \mathbb{E}$. It is preimage of canonical projection $\mathrm{pr}_{\mathbb{E}} : \mathbb{E} \times \mathbb{F} \to \mathbb{E}$, $\mathrm{pr}_{\mathbb{E}} : (x,\, f) \to x$, and by this reason, instead of pointing out the collection of all manifolds of the form $\{x\} \times \mathbb{F}$, it is sufficient to specify the projection $\mathrm{pr}_{\mathbb{E}}$. Thus, one arrives at the structure of a bundle $(\mathbb{E} \times \mathbb{F},\, \mathbb{E},\, \mathrm{pr}_{\mathbb{E}},\, \mathbb{F})$. Here $\mathbb{E} \times \mathbb{F}$ is *enhanced physical space* over the manifold of places $\mathbb{E}$, and the manifold $\mathbb{F}$ is collection of extra degrees of freedom. Enhanced physical space and conventional physical space are related via the map $\mathrm{pr}_{\mathbb{E}}$. Note, that here we take extra degrees of freedom from one manifold $\mathbb{F}$, although one may associate with each point $x \in \mathbb{E}$ some manifold $\mathbb{F}_x$, and manifolds $\mathbb{F}_x$ and $\mathbb{F}_y$ for distinct points x and y may differ. Such the case is beyond of this study.

The structure of manifold $\mathbb{F}$ may be rather general. One can consider the following particular cases. In the first case $\mathbb{F}$ is m-dimensional vector space. In the second case we deal with Lie group $(G,\, \top)$ with group operation $\top$. Elements of G are associated with orientations of points. The structure of Lie group allows to introduce the following map:

$$\lhd_{\mathbb{E}}\colon\ (\mathbb{E} \times G) \times G \to \mathbb{E} \times G, \quad (x,\, g) \lhd_{\mathbb{E}} h := (x,\, g \top h),$$

the action of Lie group G on enhanced physical space $\mathbb{E} \times G$. It defines translations along each fiber $\{x\} \times G$, i. e., one can obtain other orientations of point x from some given one.

We went into detail on the description of these cases because their differences are significant in the derivation of various models for oriented bodies, namely, micropolar, micromorphic and shell-like solids.

2. Material Manifolds

2.1. General Description for Material Manifold

3°. Body manifold. As it was mentioned at the beginning of the study, we leave the possibility for a material manifold to have the most common non-Euclidean geometry. Its formalization therefore calls for more general considerations, presented below. In what follows we use the concepts of a body, its shapes, and mappings between them. All these notions are introduced within the theory of connections on smooth manifolds [19,20]. In particular, the body, i. e., a set of material points, is formalized as a smooth manifold $\mathfrak{B}$ of dimension $n \leqslant 3$ (we refer on it as *body manifold*) [11,21]. This manifold does not carry any metric

[3] Let us dwell into the issue, how to choose inner product $(\cdot)$ and orientation or. Within framework of classical physics it is assumed that one has three rigid reference standards (one for each dimension) and rigid protractor. The reference standards are formalized by fixed three non-coplanar vectors $(\boldsymbol{i}_1,\, \boldsymbol{i}_2,\, \boldsymbol{i}_3)$ from $\mathbb{V}$. Upon measurements it is *defined* that vectors $\boldsymbol{i}_k$ have unit length, mutually orthogonal, and form right-hand triad. From formal viewpoint this means that basis $(\boldsymbol{i}_k)_{k=1}^3$ defines an inner product, with respect to which it is orthogonal: $\boldsymbol{u} \cdot \boldsymbol{v} := \delta_{mn} u^m v^n$ for $\boldsymbol{u} = u^k \boldsymbol{i}_k$ and $\boldsymbol{v} = v^k \boldsymbol{i}_k$; it defines orientation as well: $\mathrm{or} = [(\boldsymbol{i}_k)_{k=1}^3]$.

or connection and defines only topological features of the body. In this regard the body can be viewed as the following structure:

$$\mathfrak{B} = (B,\, \mathcal{T}_B,\, \mathcal{D}_B), \tag{2.1}$$

where B is the underlying set, $\mathcal{T}_B$ is a Hausdorff topology on B, that satisfies the second countability axiom, and $\mathcal{D}_B$ is a smooth structure on the topological manifold $(B, \mathcal{T}_B)$. We denote the points of $\mathfrak{B}$ by uppercase Fraktur symbols like $\mathfrak{X}$, $\mathfrak{Y}$, $\mathfrak{Z}$. It should be noted that often a structure for $\mathfrak{B}$ can be derived from the structure for some shape clearing it of Euclidean geometry. This issue will be discussed in detail further, in section 5.2.

4°. Geometry on body manifold. Vividly speaking, the body manifold is a trunk of a tree which branches represent particular spaces. The only question is which branch should be used in modelling. One can obtain the structure of *geometric space* by adding Riemannian metric, or connection, or volume form, or some of their combination, to the basic structure (2.1). Table 1 contains examples of geometric spaces[4], commonly used in geometric continuum mechanics [22–24].

Table 1

Geometric spaces over $\mathfrak{B}$

Space	Structure	Primary fields	Secondary fields
Riemann space	$(B,\, \mathcal{T}_B,\, \mathcal{D}_B,\, \mathsf{g}_B,\, \nabla_B,\, dV_B)$	g_B	$\nabla_B,\, dV_B$
Weitzenböck space	$(B,\, \mathcal{T}_B,\, \mathcal{D}_B,\, \mathsf{g}_B,\, \nabla_B,\, \mu_B)$	$\mathsf{H},\, \mu_B$	$\mathsf{g}_B,\, \nabla_B$
Weyl space	$(B,\, \mathcal{T}_B,\, \mathcal{D}_B,\, \mathsf{g}_B,\, \nabla_B,\, \mu_B)$	$\mathsf{g}_B,\, \nu,\, \mu_B$	∇_B

On Table 1 the field g_B corresponds to Riemann metric, and the field ∇_B corresponds to affine connection. The body manifold $\mathfrak{B}$ is supposed to be oriented [25] and its volume form is denoted by μ_B. The column "Primary fields" contains fields that can be prescribed from some physical reasons that don't depend on the structure of geometry. The latter column, "Secondary fields", contains fields, which can be derived from the primary ones and geometric properties of smooth manifolds. Note that if the space is Riemannian, then the volume form $\mu_B = dV_B$ is determined by metric as $dV_B = \sqrt{\det \mathsf{g}_B}\, d\mathfrak{X}^1 \wedge \cdots \wedge d\mathfrak{X}^n$. The connection ∇_B is Levi-Civita connection, being also determined by metric. The affine connection and metric of Weitzenböck space are generated by prescribed field H of linear transformations. Finally, the affine connection of Weyl space can be completely determined by 1-form ν [26].

2.2. Enhanced Material Manifold

5°. Body bundle. In this study we consider bodies, which particles are, in turn, perform themselves as continual sets, consisting of microparticles. With a view to introduce more detailed labelling for constituents of the body, one can endow the body manifold $\mathfrak{B}$ with fiber bundle structure [27,28] $(F\mathfrak{B},\, \mathfrak{B},\, \pi_{\mathfrak{B}},\, \mathbb{F})$. Here $F\mathfrak{B}$ is a smooth manifold, the total space of the bundle, to which we refer as *enhanced body*, $\mathfrak{B}$ is the original manifold of labels of particles, the base of the bundle, $\pi_{\mathfrak{B}} : F\mathfrak{B} \to \mathfrak{B}$ is a smooth surjective map, called projection, and $\mathbb{F}$ is a smooth manifold, called model fiber. Its elements serve as labels for microparticles. Submanifold $F\mathfrak{B}_{\mathfrak{X}} := \pi_{\mathfrak{B}}^{-1}(\{\mathfrak{X}\})$ is the fiber over point $\mathfrak{X}$. To stay in conventional framework of differential geometry, the following condition is required to be hold: for each point $\mathfrak{X} \in \mathfrak{B}$ there exist a neighborhood U in $\mathfrak{B}$ and a diffeomorphism $\Phi : \pi_{\mathfrak{B}}^{-1}(U) \to U \times \mathbb{F}$, called local trivialization, such that

$$\mathrm{pr}_U \circ \Phi = \pi_{\mathfrak{B}}, \tag{2.2}$$

where $\mathrm{pr}_U : U \times \mathbb{F} \to U$ is the canonical projection of the Cartesian product onto the first factor. Thus, diffeomorphism Φ has the following representation: $\Phi(p) = (\pi_{\mathfrak{B}}(p),\, \varphi(p))$, for some smooth mapping $\varphi : \pi_{\mathfrak{B}}^{-1}(U) \to \mathbb{F}$.

The local trivialization property means that enhanced body $F\mathfrak{B}$ is locally arranged as Cartesian product of some part of $\mathfrak{B}$ and the model fiber $\mathbb{F}$. This allows one to introduce special local coordinates on $F\mathfrak{B}$. Indeed, let $m = \dim \mathbb{F}$, and let $\Phi : \pi_{\mathfrak{B}}^{-1}(U) \to U \times \mathbb{F}$ be local trivialization, where U is also coordinate domain of some chart $(U,\, \sigma_{\mathfrak{B}})$ on $\mathfrak{B}$; here $\sigma_{\mathfrak{B}} : U \to \mathbb{R}^n$ is coordinate map. Moreover, let $(V,\, \sigma_{\mathbb{F}})$ be a chart on $\mathbb{F}$; here $\sigma_{\mathbb{F}} : V \to \mathbb{R}^m$ is also coordinate map. Then put $O := \Phi^{-1}(U \times V) \subset \pi_{\mathfrak{B}}^{-1}(U)$. The restriction

$$\Phi_O = \Phi|_O :\, O \to U \times V$$

is homeomorphism and by this reason[5]

$$\Sigma = (\sigma_{\mathfrak{B}} \times \sigma_{\mathbb{F}}) \circ \Phi_O :\, O \to \mathbb{R}^n \times \mathbb{R}^m, \quad \Sigma(p) = (\mathfrak{X}^1,\, ...,\, \mathfrak{X}^n;\, \mathfrak{f}^1, ..., \mathfrak{f}^m),$$

[4]More detailed description of what metric and connection give to body manifold can be found in paragraph **23°** of the Appendix.

[5]Here $f_1 \times f_2 : X_1 \times X_1 \to Y_1 \times Y_2$ is designation for product of mappings $f_i : X_i \to Y_i$, $i = 1, 2$, defined as $f_1 \times \times f_2(x_1,\, x_2) := (f_1(x_1),\, f_2(x_2))$.

is coordinate homeomorphism. Thus, (O, Σ) is a chart on enhanced body $F\mathfrak{B}$. We refer to coordinates, induced by this chart, as natural coordinates.

The chart (O, Σ) has the property, that any point p from O can be completely determined by coordinates of the base manifold $\mathfrak{B}$ and coordinates of the model fiber $\mathbb{F}$. Moreover, the coordinate representation

$$\widetilde{\pi}_{\mathfrak{B}} = \sigma_{\mathfrak{B}} \circ \pi_{\mathfrak{B}} \circ \Sigma^{-1} : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$$

of the projection $\pi_{\mathfrak{B}}$ coincides with the canonical projection of $\mathbb{R}^n \times \mathbb{R}^m$ onto $\mathbb{R}^n$.

The structure of general fiber bundle is very flexible. One can obtain particular cases by assuming that model fiber $\mathbb{F}$ is either vector space or Lie group and imposing the corresponding restrictions on local trivializations. Due to importance of these cases in our study, we discuss them individually. Examples of bundles, listed below, would be used in various theories of micropolar fields considered in the study.

6°. The case of vector bundle. Material vector bundle of rank m [19] is the fiber bundle $(V\mathfrak{B}, \mathfrak{B}, \pi_{\mathfrak{B}}, \mathbb{F})$ over $\mathfrak{B}$, where the substructure $\mathbb{F}$ is m-dimensional real vector space, which elements are orientations of the medium. It is supposed that for every $\mathfrak{X} \in \mathfrak{B}$ the preimage $\pi_{\mathfrak{B}}^{-1}(\{\mathfrak{X}\}) =: V\mathfrak{B}_{\mathfrak{X}}$ is m-dimensional real vector space. Moreover, local trivialization $\Phi : \pi_{\mathfrak{B}}^{-1}(U) \to U \times \mathbb{F}$ satisfies, beyond the property (2.2), the following requirement: for all $\mathfrak{Y} \in U$, the mapping $\Phi|_{V\mathfrak{B}_{\mathfrak{Y}}} : V\mathfrak{B}_{\mathfrak{Y}} \to \mathbb{F}$ is isomorphism between vector spaces $V\mathfrak{B}_{\mathfrak{Y}}$ and $\{\mathfrak{Y}\} \times \mathbb{F} \cong \mathbb{F}$.

Thus, like in the case of general fiber bundle, the whole enhanced body $V\mathfrak{B}$ is split into disjoint union $V\mathfrak{B} = \coprod_{x \in \mathfrak{B}} V\mathfrak{B}_{\mathfrak{X}}$ of fibers $V\mathfrak{B}_{\mathfrak{X}}$, which contain all possible material orientations of particle $\mathfrak{X}$. Since fibers $V\mathfrak{B}_{\mathfrak{X}}$ are linearly isomorphic to typical fiber $\mathbb{F}$, i. e., $V\mathfrak{B}_{\mathfrak{X}} \cong \mathbb{F}$, in reasonings one can replace them by elements of the model fiber.

The bundle structure allows one to introduce natural coordinates on $V\mathfrak{B}$. Choose some coordinates $(\mathfrak{X}^i)_{i=1}^n$ on the base manifold $\mathfrak{B}$ and choose some basis $(e_i)_{i=1}^m$ for $\mathbb{F}$. Then every point of $V\mathfrak{B}$ can be completely characterized by $(m+n)$-tuple $(\mathfrak{X}^1, ..., \mathfrak{X}^n; \mathfrak{v}^1, ..., \mathfrak{v}^m) \in \mathbb{R}^{m+n}$.

7°. The case of principal bundle. Material principal bundle with structure group G [29] is a structure $(P\mathfrak{B}, \mathfrak{B}, \pi_{\mathfrak{B}}, G, \top, \lhd_{\mathfrak{B}})$, in which $P\mathfrak{B}$, $\mathfrak{B}$, and $\pi_{\mathfrak{B}} : P\mathfrak{B} \to \mathfrak{B}$ are, as earlier, enhanced body, body manifold, and projection. The substructure $(G, \top)$ is Lie group with binary operation $\top$, and $\lhd_{\mathfrak{B}}$: $P\mathfrak{B} \times G \to P\mathfrak{B}$ is a smooth right action of the group G on manifold $P\mathfrak{B}$. The following properties are assumed:

(1) The action preserves fibers of $\pi_{\mathfrak{B}}$:

$$\forall p \in P\mathfrak{B}\, \forall g \in G : \ \pi_{\mathfrak{B}}(p \lhd_{\mathfrak{B}} g) = \pi_{\mathfrak{B}}(p).$$

(2) For every point $\mathfrak{X} \in \mathfrak{B}$ there exists a neighborhood U in $\mathfrak{B}$ and a diffeomorphism $\Phi : \pi_{\mathfrak{B}}^{-1}(U) \to U \times G$, such that $\Phi(p) = (\pi_{\mathfrak{B}}(p), \varphi(p))$, where the mapping $\varphi : \pi_{\mathfrak{B}}^{-1}(U) \to G$ is equivariant, that is,

$$\forall p \in \pi_{\mathfrak{B}}^{-1}(U)\, \forall g \in G : \ \varphi(p \lhd_{\mathfrak{B}} g) = \varphi(p) \top g.$$

Thus, material principal bundle $(P\mathfrak{B}, \mathfrak{B}, \pi_{\mathfrak{B}}, G, \top, \lhd_{\mathfrak{B}})$ is particular case of material fiber bundle $(F\mathfrak{B}, \mathfrak{B}, \pi_{\mathfrak{B}}, \mathbb{F})$. The typical fiber is "linear" in the sense that it is represented by Lie group $(G, \top)$, and Lie group structure is aligned with fiber bundle structure through group action. In particular, manifold $P\mathfrak{B}$ can be endowed with natural coordinates $(\mathfrak{X}^1, ..., \mathfrak{X}^n; \mathfrak{g}^1, ..., \mathfrak{g}^m)$. Here m is dimension of G. With respect to natural coordinates projection, as well as group action, can be represented in laconic form. Like for general case of fiber bundle, the coordinate representation of projection $\pi_{\mathfrak{B}} : P\mathfrak{B} \to \mathfrak{B}$ is canonical projection:

$$\widetilde{\pi}_{\mathfrak{B}} : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n, \quad \widetilde{\pi}_{\mathfrak{B}}(\mathfrak{X}^1, ..., \mathfrak{X}^n; \mathfrak{g}^1, ..., \mathfrak{g}^m) = (\mathfrak{X}^1, ..., \mathfrak{X}^n).$$

The coordinate representation of action $\lhd_{\mathfrak{B}}$ is the map

$$(\mathfrak{X}^1, ..., \mathfrak{X}^n; \mathfrak{g}^1, ..., \mathfrak{g}^m) \widetilde{\lhd}_{\mathfrak{B}} (\mathfrak{h}^1, ..., \mathfrak{h}^m) = (\mathfrak{X}^1, ..., \mathfrak{X}^n; (\mathfrak{g}^1, ..., \mathfrak{g}^m) \widetilde{\top} (\mathfrak{h}^1, ..., \mathfrak{h}^m)),$$

where $\widetilde{\top} : \mathbb{R}^m \times \mathbb{R}^m \to \mathbb{R}^m$ is coordinate representation of group operation $\top$.

8°. Frame bundle. If general linear group $\mathrm{GL}(n; \mathbb{R})$ is chosen as structure group, then one arrives at material frame bundle $(L\mathfrak{B}, \mathfrak{B}, \pi_{\mathfrak{B}}, \mathrm{GL}(n; \mathbb{R}), ., \lhd_{\mathfrak{B}})$, in which total space is manifold over the set

$$L\mathfrak{B} = \coprod_{\mathfrak{X} \in \mathfrak{B}} L_{\mathfrak{X}}\mathfrak{B}, \quad L_{\mathfrak{X}}\mathfrak{B} = \{(\mathsf{e}_i)_{i=1}^n \mid (\mathsf{e}_i)_{i=1}^n \text{ is a basis for } T_{\mathfrak{X}}\mathfrak{B}\},$$

the projection $\pi_{\mathfrak{B}} : L\mathfrak{B} \to \mathfrak{B}$ is defined as

$$\pi_{\mathfrak{B}}(\mathfrak{X}, (\mathsf{e}_i)_{i=1}^n) := \mathfrak{X},$$

and action $\lhd_{\mathfrak{B}}$: $L\mathfrak{B} \times \mathrm{GL}(n; \mathbb{R}) \to L\mathfrak{B}$ is

$$(\mathfrak{X}, (\mathsf{e}_i)_{i=1}^n) \lhd_{\mathfrak{B}} [\Omega^i{}_j] := (\mathfrak{X}, (\Omega^j{}_i \mathsf{e}_j)_{i=1}^n).$$

Here (.) denotes matrix product. Local trivialization Φ can be defined as follows. Choose some chart (U, σ) on body manifold $\mathfrak{B}$ and let $(\partial_i)_{i=1}^n$ be coordinate frame with respect to this chart. Then for any basis $(\mathsf{e}_i)_{i=1}^n \in L_{\mathfrak{X}}\mathfrak{B}$, $\mathfrak{X} \in \mathfrak{B}$, one has decomposition $\mathsf{e}_i = {}^\sigma\Omega^j{}_i \partial_j|_{\mathfrak{X}}$, where $[{}^\sigma\Omega^i{}_j] \in \mathrm{GL}(n;\, \mathbb{R})$. Introduce the mapping $\Phi : \pi_{\mathfrak{B}}^{-1}(U) \to U \times \mathrm{GL}(n;\, \mathbb{R})$ by equality

$$\Phi(\mathfrak{X},\, (\mathsf{e}_i)_{i=1}^n) := (\mathfrak{X},\, [{}^\sigma\Omega^i{}_j]).$$

In particular, $\varphi : \pi_{\mathfrak{B}}^{-1}(U) \to \mathrm{GL}(n;\, \mathbb{R})$ acts as $\varphi(\mathfrak{X},\, (\mathsf{e}_i)_{i=1}^n) = [{}^\sigma\Omega^i{}_j]$, which implies the equivariance property. The dimension of enhanced body $L\mathfrak{B}$ is $\dim L\mathfrak{B} = n + n^2$, and the representation on natural coordinates is of the form

$$L\mathfrak{B} \ni p \mapsto (\mathfrak{X}^1,\, ...,\, \mathfrak{X}^n;\, \mathfrak{g}^1{}_1,\, ...,\, \mathfrak{g}^n{}_n) \in \mathbb{R}^n \times \mathbb{R}^{n^2}.$$

3. Kinematic Description

3.1. Conventional Kinematics

9°. Conventional configurations and deformations. Body manifold is not directly observable to us, inhabitants of three-dimensional Euclidean space $\mathbb{E}$. One can observe shapes, that are the images of configurations. By a *configuration* [11] we mean a smooth embedding[6] $\varkappa : \mathfrak{B} \to \mathbb{E}$. Thus, we formalize shapes as images $\mathbb{S}_\varkappa = \varkappa(\mathfrak{B})$. Note, that the image $\mathbb{S}_\varkappa$ may not coincide with the whole physical space $\mathbb{E}$, even if $\mathfrak{B}$ has three dimensions. By this reason, $\varkappa$ is not invertible. To remedy the issue, one can define a new map $\widehat{\varkappa} : \mathfrak{B} \to \mathbb{S}_\varkappa$, such that $\widehat{\varkappa}(\mathfrak{X}) = \varkappa(\mathfrak{X})$. Then the new map is invertible, as desired.

Let $\varkappa_R,\, \varkappa : \mathfrak{B} \to \mathbb{E}$ be configurations which images are shapes $\mathbb{S}_R$ and $\mathbb{S}$ respectively. The change of shapes is characterized by mapping $\gamma := \widehat{\varkappa} \circ \widehat{\varkappa}_R^{-1} : \mathbb{S}_R \to \mathbb{S}$, to which we refer as *deformation*. Relations between the configurations and deformations are illustrated on Fig. 1.

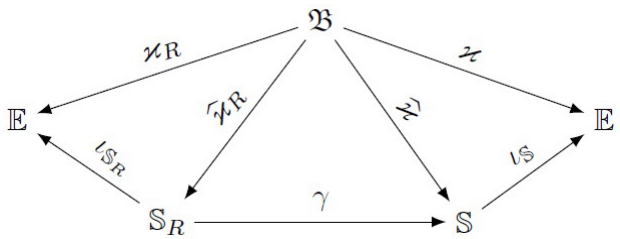

Fig. 1. Relations between the configurations and deformations

On Fig. 1, $\mathbb{S}_R = \varkappa_R(\mathfrak{B})$ and $\mathbb{S} = \varkappa(\mathfrak{B})$. The assignments $\iota_{\mathbb{S}_R} : \mathbb{S}_R \hookrightarrow \mathbb{E}$ and $\iota_{\mathbb{S}} : \mathbb{S} \hookrightarrow \mathbb{E}$ are inclusion maps[7].

10°. Motion. Suppose that we have fixed some reference shape $\mathbb{S}_R$. We define motion of the body as a family $\{\gamma_t\}_{t\in T}$ of deformations $\gamma_t : \mathbb{S}_R \to \mathbb{S}_t$, which index set $T \subset \mathbb{R}$ is an interval. This is conventional viewpoint, presented in such monographs as [31]. It is also convenient to represent the motion in terms of one smooth mapping $\gamma : \mathbb{S}_R \times T \to \mathbb{E}$ defined as $\gamma(X,\, t) := \gamma_t(X)$.

Another viewpoint on motion uses family of shapes instead of one global shape. The need of such generalization arises in the case, when body doesn't have reference shape with desired properties (in particular, stress-free), but there is a family of shapes, locally satisfying the required properties. This viewpoint is discussed in detail in section 5.1.

It is appropriate to note about the following possibility for position definition in physical space. Affine structure of physical space $\mathbb{E}$ allows to describe points through translation vectors ("vectorization"). To do this, one chooses some origin $o \in \mathbb{E}$ and defines invertible field $\mathbf{p} : \mathbb{E} \to \mathbb{V}$ of radius-vectors $\mathbf{p}(x) := \overrightarrow{ox}$. If we denote radius-vectors of points X from reference shape $\mathbb{S}_R$ by $\mathbf{X}$, i. e., $\mathbf{X} = \mathbf{p}(X)$, then we can represent mapping γ in vectorial form:

$$\boldsymbol{\chi}(\mathbf{X},\, t) := \mathbf{p}[\gamma(\mathbf{p}^{-1}(\mathbf{X}),\, t)].$$

[6] A smooth embedding from one smooth manifold M to another smooth manifold N is a mapping $\varkappa : M \to N$, which is 1) smooth, i. e., its coordinate representation is smooth in the sense of conventional Calculus; 2) at every point of M the rank of the Jacobi matrix formed upon coordinate representation of $\varkappa$ is equal to $\dim M$; 3) $\varkappa$ is a homeomorphism onto its image [25]. By requiring from configuration to be an embedding we exclude undesired situations like self-intersections.

[7] Apart formal mathematical need to use inclusion maps, there is a physical need as well. Suppose that body manifold is two-dimensional. Then one can describe its stress-strain state by means of inner geometry, i. e., using two-dimensional vectors, tensors, etc. [30]. Meanwhile, to relate fields of strains and stresses with their three-dimensional counterparts, one needs to use inclusion map. Contact of three-dimensional body with two-dimensional membrane may serve as example of such the problem.

The mapping $\boldsymbol{\chi} : \mathbb{V}_R \times T \to \mathbb{V}$, where $\mathbb{V}_R := \mathbf{p}(\mathbb{S}_R)$, is used in further considerations as well. Note the distinction between mappings γ and $\boldsymbol{\chi}$. The former mapping transforms points to points and its definition doesn't require Euclidean structure of the ambient manifold, i. e., it can be generalized to arbitrary manifolds. Meanwhile, the latter mapping transforms radius-vectors to radius-vectors an by this reason exists in Euclidean manifold only.

3.2. Enhanced Kinematics

11°. Enhanced configurations and deformations. In a manner similar to body manifold we suppose that physical manifold $\mathbb{E}$ is endowed with fiber bundle structure $(F\mathbb{E}, \mathbb{E}, \pi_{\mathbb{E}}, \mathbb{F})$ with the same model fiber $\mathbb{F}$ as for the body (in **2°** we have considered trivial bundle; here we suppose that this bundle may be of general form). Total space of the bundle $F\mathbb{E}$ plays role of enhanced physical space. Its k-dimensional submanifolds (here $k = \dim F\mathfrak{B}$) generalize conventional shapes of the body; thus, shape of the body is not only region of places, but also a collection of extra degrees of freedom.

Following the general methodology of continuum mechanics, we consider configurations and deformations as embeddings of one smooth manifold into another smooth manifold. By this reason, we define enhanced configuration as smooth embedding [15, 16] $F\varkappa : F\mathfrak{B} \to F\mathbb{E}$ of enhanced body $F\mathfrak{B}$ to enhanced physical space $F\mathbb{E}$. We suppose that this mapping preserves fibers, i. e., there exists an embedding $\varkappa : \mathfrak{B} \to \mathbb{E}$ of the body manifold to the physical space, the conventional configuration, such that

$$\varkappa \circ \pi_{\mathfrak{B}} = \pi_{\mathbb{E}} \circ F\varkappa. \tag{3.1}$$

If one introduces natural coordinates $(\mathfrak{X}^1, ..., \mathfrak{X}^n; \mathfrak{f}^1, ..., \mathfrak{f}^m)$ on enhanced body and natural coordinates $(x^1, x^2, x^3; f^1, ..., f^m)$ on enhanced physical space, then coordinate representation of $F\varkappa$ would have the form

$$\widetilde{F\varkappa}(\mathfrak{X}^1, ..., \mathfrak{X}^n; \mathfrak{f}^1, ..., \mathfrak{f}^m) = (\widetilde{\varkappa}(\mathfrak{X}^1, ..., \mathfrak{X}^n); \tau(\mathfrak{X}^1, ..., \mathfrak{X}^n; \mathfrak{f}^1, ..., \mathfrak{f}^m)),$$

where $\widetilde{\varkappa} : (\mathfrak{X}^1, ..., \mathfrak{X}^n) \mapsto (x^1, x^2, x^3)$ is a coordinate representation of configuration $\varkappa$, and $\tau : (\mathfrak{X}^1, ..., \mathfrak{X}^n; \mathfrak{f}^1, ..., \mathfrak{f}^m) \mapsto (f^1, ..., f^m)$ characterizes those part of embedding (in coordinate representation), which with material degrees of freedom associates their spatial counterpart.

Let $F\varkappa_R$, $F\varkappa : F\mathfrak{B} \to F\mathbb{E}$ be enhanced configurations, to which correspond conventional configurations $\varkappa_R$, $\varkappa : \mathfrak{B} \to \mathbb{E}$ via (3.1). Then their images $F\mathbb{S}_R = F\varkappa_R(F\mathfrak{B})$ and $F\mathbb{S} = F\varkappa(F\mathfrak{B})$ correspond to shapes of enhanced material manifold in enhanced physical space. Each of them is smooth submanifold of $F\mathbb{E}$ and one can restrict fiber bundle structure from $F\mathbb{E}$ to these shapes, i. e., to consider fiber bundles

$$(F\mathbb{S}_R, \mathbb{S}_R, \pi_{\mathbb{E}}|_{F\mathbb{S}_R}, \mathbb{F}), \quad (F\mathbb{S}, \mathbb{S}, \pi_{\mathbb{E}}|_{F\mathbb{S}}, \mathbb{F}),$$

where $\mathbb{S}_R = \varkappa_R(\mathfrak{B})$, $\mathbb{S} = \varkappa(\mathfrak{B})$ are n-dimensional submanifolds of physical space $\mathbb{E}$, that represent conventional shapes of the body. Of course, they are, in some sense, projections of enhanced shapes $F\mathbb{S}_R$ and $F\mathbb{S}$, and by this reason the information about extra variables is lost. Mappings $\pi_{\mathbb{E}}|_{F\mathbb{S}_R} : F\mathbb{S}_R \to F\mathbb{S}_R$ and $\pi_{\mathbb{E}}|_{F\mathbb{S}} : F\mathbb{S} \to F\mathbb{S}$ are restrictions of the projection $\pi_{\mathbb{E}}$ to the corresponding shapes.

Bearing in mind the intuitive meaning of deformation as change of shapes we define composition[8]

$$F\gamma = \widehat{F\varkappa} \circ \widehat{F\varkappa}_R^{-1} : F\mathbb{S}_R \to F\mathbb{S},$$

to which we refer as enhanced deformation. If $\varkappa_R, \varkappa : \mathfrak{B} \to \mathbb{E}$ are conventional configurations that correspond to enhanced ones, then the composition $\gamma = \widehat{\varkappa} \circ \widehat{\varkappa}_R^{-1} : \mathbb{S}_R \to \mathbb{S}$ is the conventional deformation, i. e., change of places. This is exactly what one observes in physical space if not using experimental setup that allows to identify extra degrees of freedom. Enhanced deformation $F\gamma$ and conventional deformation γ are related by formula analogous to (3.1):

$$\gamma \circ \pi_{\mathbb{E}}|_{F\mathbb{S}_R} = \pi_{\mathbb{E}}|_{F\mathbb{S}} \circ F\gamma. \tag{3.2}$$

Relations between shapes, configurations, deformations and their enhanced counterparts are shown on Fig. 2.

For coordinate representation of enhanced deformation choose natural coordinates[9] $(X^1, ..., X^n; F^1, ..., F^m)$ on reference shape $F\mathbb{S}_R$ and natural coordinates $(x^1, ..., x^n; f^1, ..., f^m)$ on actual shape $F\mathbb{S}$. Then coordinate representation of deformation $F\gamma$ has the form

$$\widetilde{F\gamma}(X^1, ..., X^n; F^1, ..., F^m) = (\widetilde{\gamma}(X^1, ..., X^n); \widetilde{\varepsilon}(X^1, ..., X^n; F^1, ..., F^m)).$$

[8]Like in the case of conventional configurations (see **9°**), the mappings $F\varkappa_R$ and $F\varkappa$ are not invertible in general. To define deformation as change of shape, we restrict the codomains of these mappings to the images. So obtained maps are denoted with hat signs.

[9]In these tuples, $(X^1, ..., X^n)$ are coordinates on the shape $\mathbb{S}_R$ and $(x^1, ..., x^n)$ are coordinates on the shape $\mathbb{S}$; both shapes are considered as manifolds on its own right.

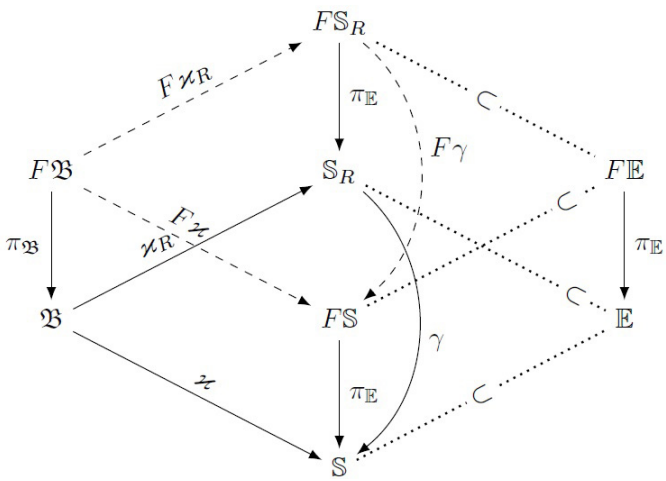

Fig. 2. Enhanced configurations and deformations

Here $\widetilde{\gamma} : (X^1, ..., X^n) \mapsto (x^1, ..., x^n)$ is coordinate representation of deformation γ, and $\widetilde{\varepsilon}(X^1, ..., X^n; F^1, ..., F^m) \mapsto (f^1, ..., f^m)$ is the mapping, which assigns with reference values of extra degrees of freedom their actual values.

Note, that in general, mapping $\widetilde{\varepsilon} : \mathbb{R}^{m+n} \to \mathbb{R}^n$ doesn't have counterpart among "point to point" mappings $F\mathbb{S}_R \to \mathbb{F}$. Meanwhile, there is a particular case, when it has such the counterpart. Suppose that the physical bundle $(F\mathbb{E}, \mathbb{E}, \pi_{\mathbb{E}}, \mathbb{F})$ is trivial, i. e., local trivialization $\Phi : \pi_{\mathbb{E}}^{-1}(U) \to U \times \mathbb{F}$ is global: $U = \mathbb{E}$. Then one can replace $F\mathbb{E}$ by $\mathbb{E} \times \mathbb{F}$ and $\pi_{\mathbb{E}}$ by canonical projection $\mathrm{pr}_{\mathbb{E}} : \mathbb{E} \times \mathbb{F} \to \mathbb{E}$. By this reason, one can consider enhanced deformation as mapping $F\gamma : \mathbb{S}_R \times \mathbb{F} \to \mathbb{S} \times \mathbb{F}$, and the condition (3.2) implies, that there exists a mapping $\varepsilon : \mathbb{S}_R \times \mathbb{F} \to \mathbb{F}$, such that

$$F\gamma(X, F) = (\gamma(X), \varepsilon(X, F)). \tag{3.3}$$

One sees, that in this case deformation of solids with extra degrees of freedom is characterized by two mappings $\gamma : \mathbb{S}_R \to \mathbb{S}$ and $\varepsilon : \mathbb{S}_R \times \mathbb{F} \to \mathbb{F}$, which, in natural coordinates, have representations $\widetilde{\gamma}$ and $\widetilde{\varepsilon}$. Defined above enhanced configurations and deformations are mathematically close to the generalized deformations introduced in [15].

12°. Sections. Mathematical structure based on the idea of embedding of an enhanced material manifold into an enhanced physical space is rather general. In particular, it allows for continual set of possible orientations, associated with a material point. To derive conventional model of oriented solid, one has to limit this set in a certain way. One possible approach is to define a section over the bundle, thereby choose a single reference orientation for each material point.

Let $(F\mathfrak{B}, \mathfrak{B}, \pi_{\mathfrak{B}}, \mathbb{F})$ be material body bundle. A smooth section of this bundle is a smooth mapping $\sigma : \mathfrak{B} \to F\mathfrak{B}$, such that $\pi_{\mathfrak{B}} \circ \sigma = \mathrm{Id}_{\mathfrak{B}}$. The latter equality means that $\sigma(\mathfrak{X}) \in F\mathfrak{B}_{\mathfrak{X}}$ for each $\mathfrak{X} \in \mathfrak{B}$. Choosing section σ, we arrive at the structure $(F\mathfrak{B}, \mathfrak{B}, \pi_{\mathfrak{B}}, \mathbb{F}, \sigma)$, to which we refer as oriented solid. In what follows we suppose that σ is an embedding. Then configuration of oriented solid is formalized as an embedding

$$F\varkappa_\sigma := F\varkappa \circ \sigma : \mathfrak{B} \to F\mathbb{E},$$

where $F\varkappa : F\mathfrak{B} \to F\mathbb{E}$ is some enhanced configuration. With regard to deformations, we obtain that the equality (3.3) takes the form

$$F\gamma_U(X) = (\gamma(X), \varepsilon(X, U_X)),$$

where γ is conventional deformation, while $\mathbb{S}_R \ni X \mapsto U_X \in \mathbb{F}$ is section of fiber bundle $(F\mathbb{S}_R, \mathbb{S}_R, \pi_{\mathbb{E}}|_{F\mathbb{S}_R}, \mathbb{F})$, induced by section σ. Thus, we arrive at the following representation for deformation of micromorphic solid:

$$F\gamma_U(X) = (\gamma(X), \widehat{\varepsilon}(X)),$$

and it means that deformation is completely characterized by mappings $\gamma : \mathbb{S}_R \to \mathbb{S}$ and $\widehat{\varepsilon} : \mathbb{S}_R \to \mathbb{F}$.

Similarly, when one deals with material vector bundle (see paragraph **24°** of the Appendix), the formula (5.10) for enhanced deformation reduces to

$$V\gamma_U(X) = (\gamma(X), \boldsymbol{\mathcal{M}}(X, U_X)),$$

or, denoting $\boldsymbol{\mathcal{M}}_U(X) := \boldsymbol{\mathcal{M}}(X, U_X)$, to

$$V\gamma_U(X) = (\gamma(X), \boldsymbol{\mathcal{M}}_U(X)). \tag{3.4}$$

Here $X \mapsto \boldsymbol{\mathcal{M}}_U(X)$ is field $\mathbb{S}_R \to \mathbb{F}$ of actual directors.

There is an issue related with the above considerations. As it is assumed, with each point X of reference shape $\mathbb{S}_R$ one associates some vector $\boldsymbol{d}_X^R$ from $\mathbb{F}$. A deformation causes change of shape and then particles of body occupy some shape $\mathbb{S}$. Orientations $\boldsymbol{d}_X^R$, in turn, deform to orientations $\boldsymbol{d}_x$, associated with points x from $\mathbb{S}$. Meanwhile, this picture depends on observer: different observers may choose different reference orientations, which can transform to different actual orientations as well. To make considerations objective, one needs to consider relations between orientations instead of the orientations themselves. But these relations are hidden in (5.10). Indeed, for each $X \in \mathbb{S}_R$ one has linear partial mapping[10] $\boldsymbol{\mathcal{M}}_X \in \mathrm{Lin}(\mathbb{F};\, \mathbb{F})$. This mapping transforms reference orientation U to actual orientation $u = \boldsymbol{\mathcal{M}}_X[U]$. If we deal with sections, then formula (3.4) should be replaced by

$$V\gamma_U(X) = (\gamma(X),\, \boldsymbol{\mathcal{M}}_X[U_X]). \tag{3.5}$$

Here $U : X \mapsto U_X$ is fixed section on reference shape, i. e., field of reference directors. Thus, in fact, deformation is completely characterized by mapping $\gamma : \mathbb{S}_R \to \mathbb{S}$, the conventional deformation, and field $\boldsymbol{\mathcal{M}} : \mathbb{S}_R \to \mathrm{Lin}(\mathbb{F};\, \mathbb{F})$ of linear maps, which relate reference and actual orientations.

Note, that since shapes $\mathbb{S}_R$ and $\mathbb{S}$ are equitable, the enhanced deformation $V\gamma$ is a diffeomorphism. This implies, in particular, that linear map $\boldsymbol{\mathcal{M}}_X$ from formula (3.5) is invertible, as well as conventional deformation γ.

4. Action Integral

4.1. Action Integral of Conventional Elasticity

13°. Classical Lagrangian. The main focus of this study is the action integral, which will be denoted with the symbol $\mathscr{J}$. We believe that $\mathscr{J}$ can be defined as the integral of a smooth scalar function of a certain set of independent and dependent variables (fields). All follow-up analysis depends upon the choice of these variables and their geometric structure (scalar, vectorial or tensorial).

For classical (non-polar) continuous medium action integral can be written in the following form:

$$\mathscr{J} = \int\limits_{t_1}^{t_2} \int\limits_{\mathbb{S}_R} \mathscr{L}\, dV\, dt, \quad \mathscr{L} = \mathscr{L}(\mathbf{X}, t, \boldsymbol{\chi}, \boldsymbol{\nabla}\boldsymbol{\chi}, \dot{\boldsymbol{\chi}}), \tag{4.1}$$

where the integration is performed over the arbitrary time interval $[t_1,\, t_2]$ and arbitrary reference domain $\mathbb{S}_R \subset \mathbb{E}$. In this expression $\mathscr{L}$ is a Lagrangian density per unit of the volume of reference shape, $\mathbf{X}$ is the position of material particle in reference shape identified with radius-vector, t is a time variable, $\boldsymbol{\chi} = \boldsymbol{\chi}(\mathbf{X}, t)$ represents positions of material particles in actual shape, and $\boldsymbol{\nabla}\boldsymbol{\chi}$ is position gradient[11].

It should be noted that, generally, the dimension of $\mathbb{S}_R$ may be less than for $\mathbb{E}$. Then instead of using three-dimensional field $\boldsymbol{\nabla}\boldsymbol{\chi}$ one needs to use two-dimensional surface gradient $\boldsymbol{\nabla}_s\boldsymbol{\chi}$ introduced in [30]. This will play a significant role in the derivations for shell-like bodies. Above all, let us make no assumption about the property of reference shape to be free from stresses.

4.2. Solids with Orientations

14°. Preliminary reasonings. Even in the framework of conventional elasticity one has to take into account that every deformation within infinitesimal neighborhood of any point X from reference shape has "rotation" part. During deformation each infinitesimal fiber emanating from X stretches and rotates according to Cauchy's polar decomposition theorem [18]: deformation gradient $\boldsymbol{\nabla}\boldsymbol{\chi}$ can be represented as the product of an orthogonal tensor $\boldsymbol{O}$ and symmetric tensor $\boldsymbol{V}$, i. e.,

$$\boldsymbol{\nabla}\boldsymbol{\chi} = \boldsymbol{V}\cdot\boldsymbol{O}, \quad \boldsymbol{O}^{\mathrm{T}} = \boldsymbol{O}^{-1}, \quad \boldsymbol{V} = \boldsymbol{V}^{\mathrm{T}} = \Big(\boldsymbol{\nabla}\boldsymbol{\chi}\cdot(\boldsymbol{\nabla}\boldsymbol{\chi})^{\mathrm{T}}\Big)^{1/2}. \tag{4.2}$$

The first equality of (4.2) implies that the tensor field $\boldsymbol{O}$ is related with actual positions $\boldsymbol{\chi}$ of particles:

$$\boldsymbol{O} = \boldsymbol{V}^{-1}\cdot\boldsymbol{\nabla}\boldsymbol{\chi} = \Big(\boldsymbol{\nabla}\boldsymbol{\chi}\cdot(\boldsymbol{\nabla}\boldsymbol{\chi})^{\mathrm{T}}\Big)^{-1/2}\cdot\boldsymbol{\nabla}\boldsymbol{\chi}. \tag{4.3}$$

Formula (4.3) shows that rotations of infinitesimal fibers are embodied in the deformation gradient and are not independent from $\boldsymbol{\chi}$: elementary volume, associated with $\mathbf{X}$, stretches and rotates as the whole; after

[10] Hereafter the symbol $\mathrm{Lin}(U;\, V)$ denotes vector space of linear maps $U \to V$.

[11] Here $\boldsymbol{\nabla}\boldsymbol{\chi}$ is considered as indivisible symbol; $\boldsymbol{\nabla}\boldsymbol{\chi} = \dfrac{\partial\chi^k}{\partial X^l}\boldsymbol{i}_k \otimes \boldsymbol{i}^l$.

deformation these volumes again constitute a connected region. The natural step is to introduce another rotations, independent from $\boldsymbol{\chi}$, and to associate them with "microparticles".

Note, that rotation of infinitesimal fiber, represented by translation vector $d\mathbf{X}$, can be determined within Rodrigues' rotation formula[12] [33]:

$$d\mathbf{X}' = \cos\theta d\mathbf{X} + \sin\theta(\boldsymbol{k}\times d\mathbf{X}) + (\boldsymbol{k}\cdot d\mathbf{X})(1-\cos\theta)\boldsymbol{k}. \tag{4.4}$$

Here $\boldsymbol{k}$ is a unit vector directed along the rotation axis and θ is rotation angle. Thus, instead of dealing with second-rank tensor field $\boldsymbol{O}$ one can deal with pair $(\theta,\, \boldsymbol{k})$, which consists of rotation angle and axis direction. To this end, we introduce vector field $\boldsymbol{\varphi_O} := \theta\boldsymbol{k}$, which we would use as a basis for the future generalization.

Let us discuss relation between rotation tensor $\boldsymbol{O}$ and pair $(\theta,\, \boldsymbol{k})$ in more detail. The following formula allows to obtain $\boldsymbol{O}$ upon pair[13] $(\theta,\, \boldsymbol{k})$:

$$\boldsymbol{O} = \cos\theta\,\mathbf{1} + (1-\cos\theta)\boldsymbol{k}\otimes\boldsymbol{k} + \sin\theta\boldsymbol{K},$$

where $\boldsymbol{K}$ is second-rank tensor such that[14] $\boldsymbol{K}\boldsymbol{v} = \boldsymbol{k}\times\boldsymbol{v}$. Conversely, suppose that $\boldsymbol{O}$ is known. To determine pair $(\theta,\, \boldsymbol{k})$, one needs to do the following steps [33]:

(1) Solve eigenvalue problem $\boldsymbol{O}\boldsymbol{k} = \boldsymbol{k}$ under condition $\|\boldsymbol{k}\| = 1$. This gives $\boldsymbol{k}$.

(2) The angle θ is obtained from the solution of equation $\sin\theta = -\dfrac{\mathrm{tr}(\boldsymbol{K}\boldsymbol{O})}{2}$.

15°. Micropolar model. Within the micropolar theory of elasticity, in contrast with conventional (symmetric) theory, it is assumed that the orientation of the elementary volume is determined independently. One introduces independent vector field $\boldsymbol{\varphi} = \boldsymbol{\varphi}(\mathbf{X}, t)$ and considers it as an additional generalized coordinate. In this case the density of Lagrangian $\mathscr{L}$ is a function of material coordinates $\mathbf{X}$, time t, fields $\boldsymbol{\chi}(\mathbf{X}, t)$, $\boldsymbol{\varphi}(\mathbf{X}, t)$ and their first gradients, i. e.

$$\mathscr{L} = \mathscr{L}(\mathbf{X}, t, \boldsymbol{\chi}, \boldsymbol{\nabla}\boldsymbol{\chi}, \dot{\boldsymbol{\chi}}, \boldsymbol{\varphi}, \boldsymbol{\nabla}\boldsymbol{\varphi}, \dot{\boldsymbol{\varphi}}). \tag{4.5}$$

Note, that vector field $\boldsymbol{\varphi_O}$, associated with orthogonal tensor $\boldsymbol{O}$ from (4.2) through Rodrigues' formula, is independent from $\boldsymbol{\varphi}$. The independent field $\boldsymbol{\varphi}$ can be regarded as a section of vector bundle (see paragraph **12°**).

16°. Generalized micropolar model. One can give the following geometric interpretation of the kinematics of the micropolar continuum. The non-deformable orthonormal trihedrons (triples of non-coplanar vectors) are associated with points of the medium, that are oriented along the base vectors in the reference state, and when the medium is deformed, change its spatial orientation. A more general interpretation may be given, when one allows these trihedrons to distort.

Suppose that one has fixed some orthonormal basis $(\boldsymbol{i}_k)_{k=1}^3$. Then for every trihedron $(\boldsymbol{d}_k)_{k=1}^3$ of non-coplanar vectors there exists invertible linear map $\boldsymbol{L} : \mathbb{V} \to \mathbb{V}$, such that $\boldsymbol{L}[\boldsymbol{i}_k] = \boldsymbol{d}_k$. In dyadic representation, $\boldsymbol{L} = \boldsymbol{d}_k \otimes \boldsymbol{i}^k$. Thus, instead of deformable trihedrons one can consider invertible linear maps, which are elements of general linear group. Meanwhile, the following issue arise here. The physical space $\mathbb{E}$ is too narrow to contain simultaneously places of particles and linear operators, associated with them. If we think of shapes, as of sets, which elements are pairs $(X,\, \boldsymbol{L})$, then these sets cannot be defined as

[12] One can obtain another version of formula (4.4). If put $\tau = \tan\frac{\theta}{2}$, then from (4.4) directly follows that

$$d\mathbf{X}' = \frac{1}{1+\tau^2}\left[(1-\tau^2)d\mathbf{X} + 2\tau(\boldsymbol{k}\times d\mathbf{X}) + 2\tau^2(\boldsymbol{k}\cdot d\mathbf{X})\boldsymbol{k}\right].$$

After some algebraic transformations one gets [32]

$$d\mathbf{X}' = d\mathbf{X} + \frac{1}{1+\frac{1}{4}\vartheta^2}\boldsymbol{\vartheta}\times\left(d\mathbf{X} + \frac{1}{2}\boldsymbol{\vartheta}\times d\mathbf{X}\right),$$

where $\boldsymbol{\vartheta} = 2\tau\boldsymbol{k}$, $\vartheta = \|\boldsymbol{\vartheta}\| = 2\tau$. The vector $\boldsymbol{\vartheta}$ is usually called as finite rotation vector, although its magnitude have no common with real rotation angle.

[13] If some orthonormal basis $(\boldsymbol{i}_s)_{s=1}^3$ in $\mathbb{V}$ has chosen, then, according to (4.4), operator $\boldsymbol{O}$ is represented by matrix

$$[\boldsymbol{O}] = \left(\begin{array}{c|c|c} (1-\cos\theta)k_1^2+\cos\theta & k_1k_2(1-\cos\theta)-k_3\sin\theta & k_1k_3(1-\cos\theta)+k_2\sin\theta \\ k_1k_2(1-\cos\theta)+k_3\sin\theta & (1-\cos\theta)k_2^2+\cos\theta & k_2k_3(1-\cos\theta)-k_1\sin\theta \\ k_1k_3(1-\cos\theta)-k_2\sin\theta & k_2k_3(1-\cos\theta)+k_1\sin\theta & (1-\cos\theta)k_3^2+\cos\theta \end{array}\right),$$

where k_1, k_2, k_3 are components of $\boldsymbol{k}$.

[14] In matrix form $\boldsymbol{K}$ is given by

$$[\boldsymbol{K}] = \begin{pmatrix} 0 & -k_3 & k_2 \\ k_3 & 0 & -k_1 \\ -k_2 & k_1 & 0 \end{pmatrix}.$$

images of embeddings to physical space. Usually one employs the artificial construction, when "shape" is a region of physical space, while linear operators are considered separately, being associated with each point of this region. This reasoning is suitable for conventional problems, but hardly suitable to situations when one considers incompatible deformations. To use methodology of non-Euclidean shape one needs to introduce somehow shapes, that contain places and linear operators simultaneously.

To fix the issue it seems appropriate to consider enhanced physical space $L\mathbb{E}$, which is the total space of frame bundle $(L\mathbb{E},\, \mathbb{E},\, \pi_{\mathbb{E}},\, \mathrm{GL}(3;\, \mathbb{R}),\, .,\, \lhd_{\mathbb{E}})$ discussed in paragraph **8°**. In this case configuration can be defined in usual manner as embedding $\kappa : \mathfrak{B} \to L\mathbb{E}$ and images of configurations are shapes of the body. This viewpoint is systematically developed in [34].

Any configuration $\kappa : \mathfrak{B} \to L\mathbb{E}$ defines an embedding $\varkappa : \mathfrak{B} \to \mathbb{E}$, conventional configuration, as follows: $\varkappa := \pi_{\mathbb{E}} \circ \kappa$. Thus, one indeed deals with enhanced picture, which contains all information about places of points. In the particular case, when $L\mathbb{E} = \mathbb{E} \times \mathrm{GL}(3;\, \mathbb{R})$, one has the following representation for κ: $\kappa(\mathfrak{X}) = (\varkappa(\mathfrak{X});\, \boldsymbol{L}(\mathfrak{X}))$. Here $\varkappa : \mathfrak{B} \to \mathbb{E}$ is conventional configuration and $\boldsymbol{L} : \mathfrak{B} \to \mathrm{GL}(3;\, \mathbb{R})$ corresponds to field of trihedrons.

If one chooses natural coordinates on $L\mathbb{E}$, generated by coordinate map $\varphi_{L\mathbb{E}} : L\mathbb{E} \to \mathbb{R}^3 \times \mathbb{R}^9$, and some coordinates on the body manifold $\mathfrak{B}$, generated by coordinate map $\varphi_{\mathfrak{B}} : \mathfrak{B} \to \mathbb{R}^n$, then coordinate representation of configuration $\kappa : \mathfrak{B} \to L\mathbb{E}$ is composition

$$\widetilde{\kappa} = \varphi_{L\mathbb{E}} \circ \kappa \circ \varphi_{\mathfrak{B}}^{-1}, \quad \widetilde{\kappa}(\mathfrak{X}^1,\, ...,\, \mathfrak{X}^n) = (\widetilde{\varkappa}^i(\mathfrak{X}^1,\, ...,\, \mathfrak{X}^n);\, [L]^i{}_j(\mathfrak{X}^1,\, ...,\, \mathfrak{X}^n)),$$

where $i,\, j = 1,\, 2,\, 3$ and $\widetilde{\varkappa} : \mathbb{R}^n \to \mathbb{R}^3$, $[L] : \mathbb{R}^n \to \mathbb{R}^9$ are some mappings, uniquely defined by κ. Moreover, $\widetilde{\varkappa}$ is coordinate representation for $\varkappa$: $\widetilde{\varkappa} = \varphi_{\mathbb{E}} \circ \varkappa \circ \varphi_{\mathfrak{B}}^{-1}$, where $\varphi_{\mathbb{E}} : \mathbb{E} \to \mathbb{R}^3$ is coordinate map for physical space.

With a view to describe micropolar body with incompatible deformations in the framework of geometric continuum mechanics one needs to enhance the body manifold as well, since origin of incompatibility is more general here, as it involves particles and trihedrons, while body manifold contains information of particles only. Thus, one arrives at the frame bundle $(L\mathfrak{B},\, \mathfrak{B},\, \pi_{\mathfrak{B}},\, \mathrm{GL}(n;\, \mathbb{R}),\, .,\, \lhd_{\mathfrak{B}})$. In this case embeddings $L\varkappa : L\mathfrak{B} \to L\mathbb{E}$ represent enhanced configurations[15] (see paragraph **25°** of the Appendix). Within suitable coordinates, $L\varkappa$ is represented as mapping $\widetilde{L\varkappa} = \varphi_{L\mathbb{E}} \circ L\varkappa \circ \varphi_{L\mathfrak{B}}^{-1}$, where $\varphi_{L\mathfrak{B}} : L\mathfrak{B} \to \mathbb{R}^n \times \mathbb{R}^9$ is coordinate map on total space $L\mathfrak{B}$. All above reasonings are illustrated on Fig. 3. The dashed lines from $L\mathfrak{B}$ illustrate that this part

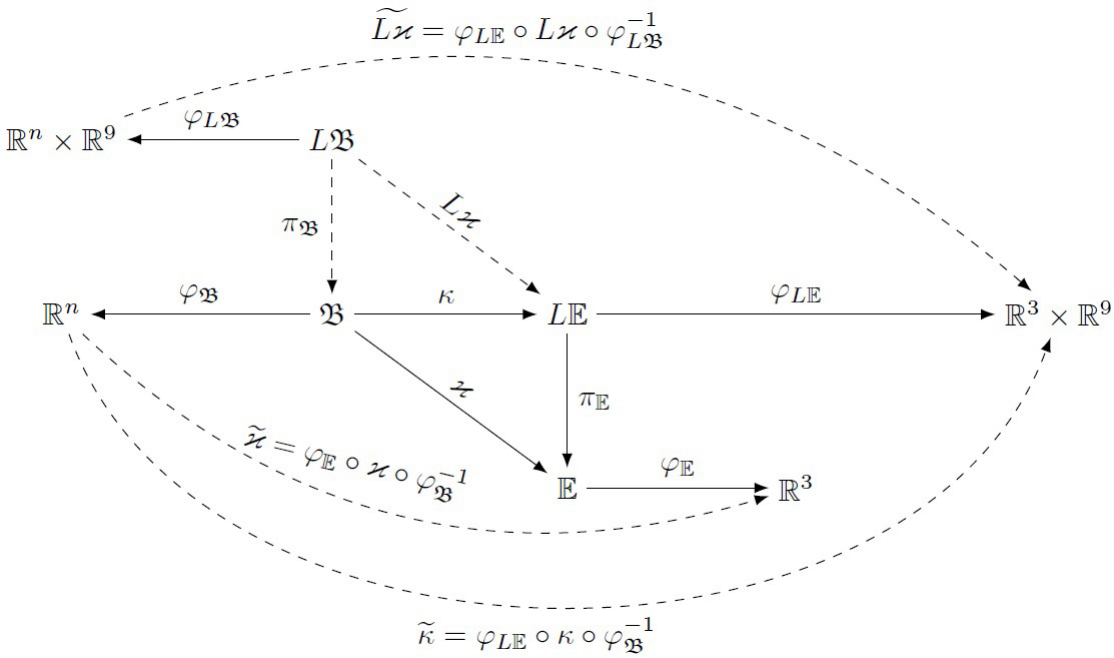

Fig. 3. Embedding of generalized micropolar body into enhanced physical space

of the figure corresponds to the case of incompatible deformations. One can obtain the conventional case of micropolar continuum if replaces general linear group $\mathrm{GL}(3;\, \mathbb{R})$ by special orthogonal group $\mathrm{SO}(3)$.

17°. Micromorphic model. In reasonings of paragraph **16°** we have associated with each particle some invertible linear transformation $\boldsymbol{L} : \mathbb{V} \to \mathbb{V}$, which is a counterpart for deformable trihedron of directors.

[15] It would be too restrictive to assume that embedding $L\varkappa$ is related with configuration $\kappa : \mathfrak{B} \to L\mathbb{E}$ as $L\varkappa = \kappa \circ \pi_{\mathfrak{B}}$. Indeed, in this case the image $L\varkappa(L\mathfrak{B})$ would be a surface in $L\mathbb{E}$, not an open set.

Within this formalism, a motion of such the solid is represented by pair $(\varkappa(\mathfrak{X}, t), \boldsymbol{L}(\mathfrak{X}, t))$, in which $\varkappa : \mathfrak{B}\times\times]t_1, t_2[\to \mathbb{E}$ is family of conventional configurations and $\boldsymbol{L} : \mathfrak{B}\times]t_1, t_2[\to \mathrm{GL}(3; \mathbb{R})$ is family of linear maps. Meanwhile, one can adopt another point of view. First, one can choose reference directors from some m-dimensional Euclidean vector space $\mathbb{F}$ instead of choosing them from translation vector space $\mathbb{V}$. In actual picture one still observes trihedrons of vectors from $\mathbb{V}$. Second, one can suppose that relation between abstract directors, i. e., vectors from $\mathbb{F}$, and real directors, i. e., vectors from $\mathbb{V}$, is linear. The corresponding linear transformation is defined by a second-rank tensor $\boldsymbol{\mathcal{X}} = \boldsymbol{\mathcal{X}}(\mathbf{X}, t) \in \mathrm{Lin}(\mathbb{F}; \mathbb{V})$, operating in a m-dimensional Euclidean vector space $\mathbb{F}$. This tensor is referred to as the tensor of microdeformations[16].

In view of the above, the density of Lagrangian can be described as:

$$\mathscr{L} = \mathscr{L}(\mathbf{X}, t, \boldsymbol{\chi}, \boldsymbol{\nabla}\boldsymbol{\chi}, \dot{\boldsymbol{\chi}}, \boldsymbol{\mathcal{X}}, \boldsymbol{\nabla}\boldsymbol{\mathcal{X}}, \dot{\boldsymbol{\mathcal{X}}}). \tag{4.6}$$

It seems appropriate to mention about relation between field $\boldsymbol{\mathcal{X}} : \mathbb{S}_R \to \mathrm{Lin}(\mathbb{F}; \mathbb{V})$, the argument of Lagrangian density (4.6), and field $\boldsymbol{\mathcal{M}} : \mathbb{S}_R \to \mathrm{Lin}(\mathbb{F}; \mathbb{F})$ from (3.5). Values of both fields are linear maps that transform reference orientations to actual orientations. It is assumed here that orientations are vectors from some abstract vector space $\mathbb{F}$. Meanwhile, in conventional theories of elasticity orientations are considered to be visible deformable trihedrons of translation vectors, i. e., elements from $\mathbb{V}$. By this reason, we suppose the following relation between fields $\boldsymbol{\mathcal{X}}$ and $\boldsymbol{\mathcal{M}}$: $\boldsymbol{\mathcal{X}} = \mathrm{In} \circ \boldsymbol{\mathcal{M}}$. Here $\mathrm{In} : \mathbb{S}_R \to \mathrm{Lin}(\mathbb{F}; \mathbb{V})$ is field of linear mappings, that perform inclusion of abstract orientations from $\mathbb{F}$ into visible elements from $\mathbb{V}$. The form of this field depends on physical nature of the model.

There is another way of justifying microdeformations, when one considers particles as aggregates, that consist of microparticles [35]. The body manifold $\mathfrak{B}$ contains labels of particles and its structure is too narrow to fit microparticles also. By this reason, suppose that each particle can be formalized as 3-dimensional Euclidean vector space $\mathbb{F}$, which, in turn, contains labels of microparticles, and introduce material vector bundle $(V\mathfrak{B}, \mathfrak{B}, \pi_{\mathfrak{B}}, \mathbb{F})$ over $\mathfrak{B}$. Here each fiber $V\mathfrak{B}_{\mathfrak{X}}$ over $\mathfrak{X} \in \mathfrak{B}$ represents single cell, associated with label $\mathfrak{X}$. The distinction between particles and microparticles requires to introduce two types of configurations. The first type is conventional configuration represented by embedding $\varkappa : \mathfrak{B} \to \mathbb{E}$, $\mathfrak{X} \mapsto \varkappa(\mathfrak{X})$, associated with particles. The second type, for $\mathfrak{X} \in \mathfrak{B}$, is an embedding $\varkappa^{\mathbb{F}}_{\mathfrak{X}} : \mathbb{F} \to \mathbb{V}$, $\boldsymbol{U} \mapsto \varkappa^{\mathbb{F}}_{\mathfrak{X}}(\boldsymbol{U})$. We suppose the following calibration condition: $\varkappa^{\mathbb{F}}_{\mathfrak{X}}(\mathbf{0}) = \mathbf{0}$. Then embedding $\varkappa^{\mathbb{F}}_{\mathfrak{X}}$ can be interpreted as assignment, that returns radius-vectors of microparticles within center of mass of the single cell $\mathfrak{X}$.

Note, that one cannot think of $\varkappa^{\mathbb{F}}_{\mathfrak{X}}$ as of embedding into physical manifold $\mathbb{E}$, since in this case there would not be clear distinction between particles and microparticles. Instead of this, one can treat microparticles as infinitesimal translation vectors emanating from center of mass of the cell $\varkappa(\mathfrak{X})$.

As it was mentioned, one cannot consider positions of particles and microparticles in physical space $\mathbb{E}$ simultaneously. Meanwhile, using vector bundles again, one can introduce vector bundle $V\mathbb{E}$ over $\mathbb{E}$ with model fiber $\mathbb{V}$. Then place and "microplace" can be unified into a single point from $V\mathbb{E}$. Both mapping $\varkappa$ and the family $(\varkappa^{\mathbb{F}}_{\mathfrak{X}})_{\mathfrak{X}\in\mathfrak{B}}$ of mappings induce global map $V\varkappa : V\mathfrak{B} \to V\mathbb{E}$, i. e., enhanced configuration, from manifold $V\mathfrak{B}$ to manifold $V\mathbb{E}$. In what follows we suppose that $V\mathfrak{B} = \mathfrak{B} \times \mathbb{F}$ and $V\mathbb{E} = \mathbb{E} \times \mathbb{V}$, i. e., vector bundles over $\mathfrak{B}$ and $\mathbb{E}$ are trivial.

To get conventional picture, described by Mindlin [35], one can provide the following modeling. As enhanced configuration is completely defined by mappings $\varkappa$ and $\varkappa^{\mathbb{F}}_{\mathfrak{X}}$, we can deal only with them. Introduce the mapping $\overline{\varkappa} : \mathfrak{B} \times \mathbb{F} \to \mathbb{E}$ by the relation

$$\overline{\varkappa}(\mathfrak{X}, \boldsymbol{U}) := \varkappa(\mathfrak{X}) + \varkappa^{\mathbb{F}}_{\mathfrak{X}}(\boldsymbol{U}).$$

This mapping returns fictive position of microparticle, equal to the sum of position of the corresponding cell and relative position of microparticle within the cell. Consider first order Taylor expansion of $\varkappa^{\mathbb{F}}_{\mathfrak{X}}(\boldsymbol{U})$: $\varkappa^{\mathbb{F}}_{\mathfrak{X}}(\boldsymbol{U}) = \varkappa^{\mathbb{F}}_{\mathfrak{X}}(\mathbf{0}) + \boldsymbol{\mathcal{X}}_{\mathfrak{X}}(\boldsymbol{U}) + \boldsymbol{o}(\|\boldsymbol{U}\|)$. Here $\boldsymbol{\mathcal{X}}_{\mathfrak{X}} : \mathbb{F} \to \mathbb{V}$ is linear map. Taking into account the calibration condition, one gets

$$\overline{\varkappa}(\mathfrak{X}, \boldsymbol{U}) := \varkappa(\mathfrak{X}) + \boldsymbol{\mathcal{X}}_{\mathfrak{X}}(\boldsymbol{U}) + \boldsymbol{o}(\|\boldsymbol{U}\|).$$

Thus, with up to $\boldsymbol{o}(\|\boldsymbol{U}\|)$, the fictive position of microparticle is defined by pair $(\varkappa, \boldsymbol{\mathcal{X}})$, where $\varkappa : \mathfrak{B} \to \mathbb{E}$ is conventional configuration and $\boldsymbol{\mathcal{X}} : \mathfrak{B} \times \mathbb{F} \to \mathbb{V}$ is tensor field of microdeformations. Therefore, the density of Lagrangian has the form (we identify body manifold with some of its shapes):

$$\mathscr{L} = \mathscr{L}(\mathbf{X}, \boldsymbol{U}, t, \boldsymbol{\chi}, \boldsymbol{\nabla}\boldsymbol{\chi}, \dot{\boldsymbol{\chi}}, \boldsymbol{\mathcal{X}}, \boldsymbol{\nabla}\boldsymbol{\mathcal{X}}, \dot{\boldsymbol{\mathcal{X}}}).$$

[16] Let us make more clear the distinction between models discussed in paragraphs **16°** and **17°**. Linear maps in them play different roles:

- In **16°** linear map is a counterpart for directors triad;
- In **17°** linear map relates family $(\boldsymbol{f}_I)_{I=1}^m$ of abstract reference directors with family $(\boldsymbol{d}_i)_{i=1}^3$ of their spatial counterpart.

Believing that Lagrangian density is independent of $\boldsymbol{U}$, *i. e.*, cells are homogeneous and isotropic, we arrive at (4.6). If the cell, above that, is absolutely rigid, the equations are reduced to the equations of the micropolar continuum (4.5).

Reasonings, provided so far, are illustrated on Fig. 4. On the figure: $\varphi_{\mathbb{F}}$, $\varphi_{V\mathfrak{B}}$, $\varphi_{\mathfrak{B}}$, $\varphi_{\mathbb{V}}$ and $\varphi_{\mathbb{E}}$ are

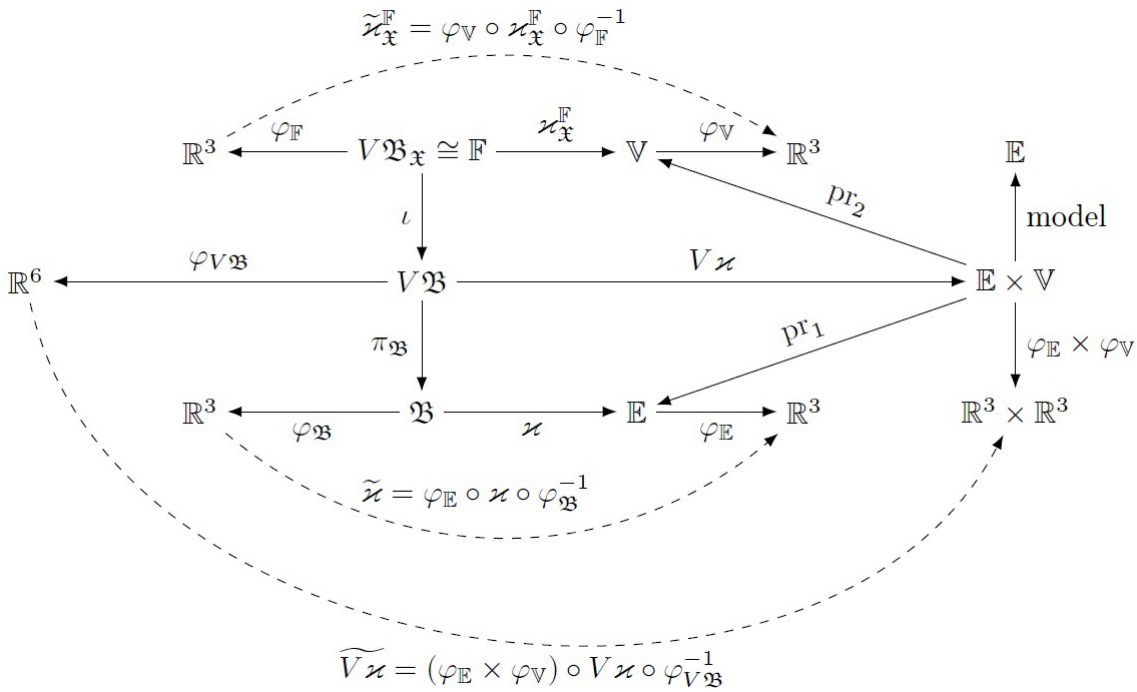

Fig. 4. Embedding of micromorphic body into physical space

coordinate mappings of manifolds indicated in lower indices. Mappings $\widetilde{\varkappa}^{\mathbb{F}}_{\mathfrak{X}}$, $\widetilde{\varkappa}$ and $\widetilde{V\varkappa}$ are coordinate representations of the corresponding mappings $\varkappa^{\mathbb{F}}_{\mathfrak{X}}$, $\varkappa$ and $V\varkappa$. The mapping ι is inclusion map. The word "model" on the right upper part of the figure indicates the transition from enhanced configuration $V\varkappa$ to fictive configuration $\overline{\varkappa}$.

18°. Shell models. Although there are many distinct models of shells, the fiber bundle formalism allows to think of these models as one. To this end a shell can be formalized as material fiber bundle $(F\mathfrak{B}, \mathfrak{B}, \pi_{\mathfrak{B}}, \mathbb{F})$ where total space $F\mathfrak{B}$ is smooth manifold of dimension 3 and base $\mathfrak{B}$ has dimension 2. The manifold $F\mathfrak{B}$ contains all labels of shell particles, while manifold $\mathfrak{B}$ contains labels of points from reduction surface. Every fiber $F\mathfrak{B}_{\mathfrak{X}}$, one-dimensional manifold, consists of material transversal elements of the shell over point $\mathfrak{X}$.

In physical space $\mathbb{E}$ one observes shape $\widehat{\mathbb{S}}$ of the shell, the image of embedding $\kappa : F\mathfrak{B} \to \mathbb{E}$, and shape $\mathbb{S}$ of the body $\mathfrak{B}$, the image of embedding $\varkappa : \mathfrak{B} \to \mathbb{E}$. In general, κ and $\varkappa$ are independent and shape $\mathbb{S}$ may not be contained in $\widehat{\mathbb{S}}$. We refer to the shape $\mathbb{S}$ as reduction surface. Let $\varphi_{F\mathfrak{B}} : F\mathfrak{B} \to \mathbb{R}^3$ be coordinate map, that returns natural coordinates of points from $F\mathfrak{B}$. That is, for $p \in F\mathfrak{B}$ one has triple $(\mathfrak{X}^1, \mathfrak{X}^2, \xi) \in \mathbb{R}^3$, where $(\mathfrak{X}^1, \mathfrak{X}^2)$ are coordinates on the manifold $\mathfrak{B}$ and ξ is "transversal" coordinate, i. e., coordinate on model fiber $\mathbb{F}$. Let $\widehat{\kappa} : F\mathfrak{B} \to \widehat{\mathbb{S}}$ be mapping, that obtained from κ by restriction of codomain (see **9°**). Then define coordinate map $\varphi_{\widehat{\mathbb{S}}} : \widehat{\mathbb{S}} \to \mathbb{R}^3$ as $\varphi_{\widehat{\mathbb{S}}} = \varphi_{F\mathfrak{B}} \circ \widehat{\kappa}^{-1}$. Thus, points from shape $\widehat{\mathbb{S}}$ are represented by tuples $(\mathfrak{X}^1, \mathfrak{X}^2, \xi)$.

One arrives at the following general vectorial relation between positions of points from $\widehat{\mathbb{S}}$ and natural coordinates on $F\mathfrak{B}$:

$$\boldsymbol{r} = \boldsymbol{f}(\mathfrak{X}^1, \mathfrak{X}^2; \xi), \tag{4.7}$$

where $\boldsymbol{f}$ depends on the model chosen for description of configuration. The semicolon separates coordinates on reduction surface from transversal coordinate. If one assumes that transversal elements are associated with normal elements, then one gets the following approximation for configuration κ: $\boldsymbol{r} = \boldsymbol{\rho}(\mathfrak{X}^1, \mathfrak{X}^2) + \xi\, \boldsymbol{n}(\mathfrak{X}^1, \mathfrak{X}^2)$, where $\boldsymbol{\rho}(\mathfrak{X}^1, \mathfrak{X}^2)$ is position vector of reduction surface and $\boldsymbol{n}$ is unit normal vector field.

In general, the choice of particular approximation for (4.7) is provided in two stages. One pulls out the reduction surface $\mathbb{S}$ from $\widehat{\mathbb{S}}$ and considers it as base manifold for some vector bundle $(V\mathbb{S}, \mathbb{S}, \pi_{\mathbb{S}}, \mathbb{F}_1)$ with model fiber $\mathbb{F}_1$, an m-dimensional vector space. Elements of the space $\mathbb{F}_1$ serve as objects, which are used to approximate partial field $\boldsymbol{f}(\mathfrak{X}^1, \mathfrak{X}^2; \cdot) : \xi \mapsto \boldsymbol{f}(\mathfrak{X}^1, \mathfrak{X}^2; \xi)$. In particular, one may consider some functional Hilbert space. Choosing some basis, e.g., Legendre polynomials, one then restricts its attention in linear

span of dimension m. This is what exactly $\mathbb{F}_1$ is. In the next step one combines fields $\boldsymbol{f}(\cdot;\,\xi):\,(\mathfrak{X}^1,\,\mathfrak{X}^2)\mapsto \boldsymbol{f}(\mathfrak{X}^1,\,\mathfrak{X}^2;\,\xi)$ and $\boldsymbol{f}(\mathfrak{X}^1,\,\mathfrak{X}^2;\,\cdot):\,\xi\mapsto \boldsymbol{f}(\mathfrak{X}^1,\,\mathfrak{X}^2;\,\xi)$ into one global field from $\mathbb{R}^3$ to $\mathbb{E}$. The image of this field is denoted by $\overline{\mathbb{S}}$. The obtained field is the result of approximation. It is expected that after modeling $\widehat{\mathbb{S}}=\overline{\mathbb{S}}$, but it is worth to note, that the shape $\overline{\mathbb{S}}$ is not the image of embedding from $F\mathfrak{B}$.

Suppose that $(e_k)_{k=1}^{\infty}$ is some Schauder basis of Hilbert space $L^2[-1,\,1]$ (not necessary orthonormal). Choosing $m\in\mathbb{N}$, we replace $\boldsymbol{f}$ from (4.7) by additive decomposition $\boldsymbol{r}=\boldsymbol{\rho}(\mathfrak{X}^1,\,\mathfrak{X}^2)+\boldsymbol{\rho}_1(\mathfrak{X}^1,\,\mathfrak{X}^2;\,\xi)$, where $\boldsymbol{\rho}_1(\mathfrak{X}^1,\,\mathfrak{X}^2;\,\xi)=\sum_{k=1}^{m}\boldsymbol{c}_k(\mathfrak{X}^1,\,\mathfrak{X}^2)e_k(\xi)$. Thus,

$$\boldsymbol{r}=\boldsymbol{\rho}(\mathfrak{X}^1,\,\mathfrak{X}^2)+\sum_{k=1}^{m}\boldsymbol{c}_k(\mathfrak{X}^1,\,\mathfrak{X}^2)e_k(\xi).$$

Here $\boldsymbol{c}_k(\mathfrak{X}^1,\,\mathfrak{X}^2)$ are vectorial coefficients of the expansion, which components define elements from vector space $\mathbb{F}_1$.

All reasonings provided above are illustrated on Fig. 5. On the figure, symbols φ with lower indices

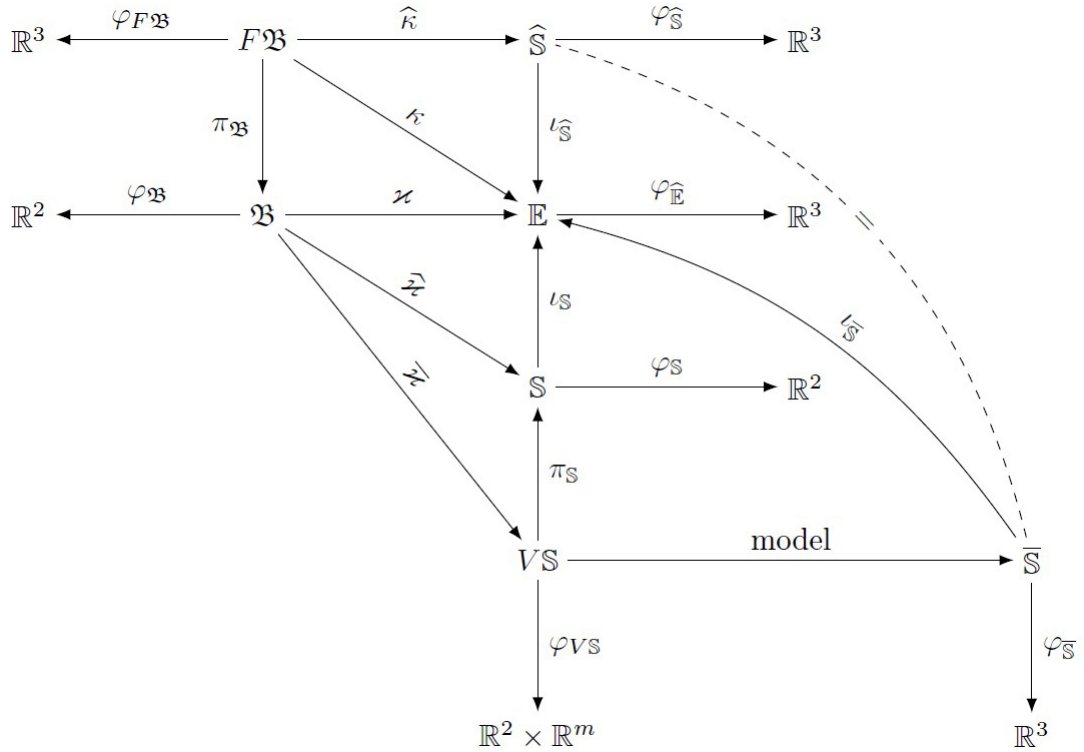

Fig. 5. Shell modeling scheme

denote the corresponding coordinate maps. Mappings ι are inclusion maps and "model" denotes the process of transition from manifold $V\mathbb{S}$ to the manifold $\overline{\mathbb{S}}$.

5. Incompatible Deformations

5.1. Local Discharging

19°. Family of shapes. In conventional elasticity one assumes that body $\mathfrak{B}$ has stress-free shape $\mathbb{S}_R$ in Euclidean physical space $\mathbb{E}$. Like all other shapes, this shape is considered as a subspace of physical manifold, with metric and connection induced from it:

$$\mathbb{S}_R=(S_R,\,\mathcal{T}_E|_{S_R},\,\mathcal{D}_E|_{S_R},\,\boldsymbol{g}_E|_{S_R},\,\nabla_E|_{S_R}).$$

Here S_R is the underlying set of the shape, while other elements of the tuple are, respectively, topology, smooth structure, metric and connection of Euclidean space $\mathbb{E}$ induced to S_R. In this case deformation is a mapping

$$\gamma:\,(S_R,\,\mathcal{T}_E|_{S_R},\,\mathcal{D}_E|_{S_R},\,\boldsymbol{g}_E|_{S_R},\,\nabla_E|_{S_R})\to(S,\,\mathcal{T}_E|_{S},\,\mathcal{D}_E|_{S},\,\boldsymbol{g}_E|_{S},\,\nabla_E|_{S}),$$

between two open (hereafter we consider the case $\dim\mathfrak{B}=3$) submanifolds of $\mathbb{E}$ with Euclidean geometry.

If solid has defects, e.g., dislocations, disclinations, etc., then the assumption of existence of *global* Euclidean stress-free shape fails. Before stating weaker assumption, let us provide auxiliary consideration.

Suppose that one have chosen some shape $\mathbb{S}_I$ in Euclidean physical space $\mathbb{E}$, the image of configuration $\varkappa_I : \mathfrak{B} \to \mathbb{E}$. We refer to it as *intermediate shape*. Moreover, let $\mathbb{S}_R$ and $\mathbb{S}$ be, respectively, reference and actual shapes in $\mathbb{E}$, which are images of configurations $\varkappa_R, \varkappa : \mathfrak{B} \to \mathbb{E}$ respectively. The shape $\mathbb{S}_R$ is assumed to be stress-free, while $\mathbb{S}_I$ and $\mathbb{S}$ are self-stressed in general. Define maps

$$\chi = \varkappa \circ \widehat{\varkappa}_I^{-1} : \mathbb{S}_I \to \mathbb{S}, \quad \xi = \varkappa_R \circ \widehat{\varkappa}_I^{-1} : \mathbb{S}_I \to \mathbb{S}_R,$$

which are deformations from the intermediate shape to actual and reference shapes respectively. Then ξ corresponds to relaxation from the shape $\mathbb{S}_I$ to the shape $\mathbb{S}_R$, and the composition $\gamma = \chi \circ \xi^{-1} : \mathbb{S}_R \to \mathbb{S}$ is the conventional deformation from stress-free reference shape to the actual shape.

Instead of considering motion $\gamma : \mathbb{S}_R \times [t_0, t_1] \to \mathbb{E}$ as a field variable, one can choose mappings $\chi : \mathbb{S}_I \times \times [t_0, t_1] \to \mathbb{E}$ and $\xi : \mathbb{S}_I \times [t_0, t_1] \to \mathbb{E}$, defined on $\mathbb{S}_I$, to be field variables. Thus, the Lagrangian density in (4.1) is replaced by the following function:

$$\mathscr{L} = \mathscr{L}(X, t, \chi, \boldsymbol{\nabla}\chi, \dot{\chi}, \xi, \boldsymbol{\nabla}\xi, \dot{\xi}). \tag{5.1}$$

Assuming independence on rigid translations, one can replace (5.1) by

$$\mathscr{L} = \mathscr{L}(X, t, \boldsymbol{\nabla}\chi, \dot{\chi}, \boldsymbol{\nabla}\xi, \dot{\xi}). \tag{5.2}$$

Independence on rigid rotations, in turn, allows to replace (5.2) by

$$\mathscr{L} = \mathscr{L}(X, t, \boldsymbol{B}, \dot{\chi}, \boldsymbol{\beta}, \dot{\xi}). \tag{5.3}$$

In (5.3) $\boldsymbol{B}$ and $\boldsymbol{\beta}$ are, respectively, $\boldsymbol{B} = \boldsymbol{\nabla}\chi\boldsymbol{\nabla}\chi^{\mathrm{T}}$ and $\boldsymbol{\beta} = \boldsymbol{\nabla}\xi\boldsymbol{\nabla}\xi^{\mathrm{T}}$.

Now, bearing in mind the auxiliary consideration, consider the case, when all Euclidean shapes of the body are self-stressed. We suppose the weaker assumption, to which we refer as *principle of local discharging*: there exist a shape $\mathbb{S}_I$ in Euclidean space and a family $(\gamma^{(X)})_{X\in\mathbb{S}_I}$ of deformations $\gamma^{(X)} : \mathbb{S}_I \to \mathbb{S}^{(X)}$ from the shape $\mathbb{S}_I$ to some shapes $\mathbb{S}^{(X)}$, such that the infinitesimal neighborhood of point $\gamma^{(X)}(Y)|_{Y=X}$ is stress-free for any $X \in \mathbb{S}_I$.

For each deformation $\gamma^{(X)}$ one can obtain deformation gradient $\boldsymbol{F}^{(X)} = \boldsymbol{\nabla}\gamma : \mathbb{S}_I \to \mathrm{Lin}(\mathbb{V}; \mathbb{V})$, $\boldsymbol{F}^{(X)} : Y \mapsto \boldsymbol{F}^{(X)}_Y$. Due to the principle of local discharging, tensor field $\boldsymbol{F}^{(X)}$ satisfies the following property: the linear map $\boldsymbol{F}^{(X)}_Y|_{Y=X} : \mathbb{V} \to \mathbb{V}$ transforms infinitesimal neighborhood of point $X \in \mathbb{S}_I$ to infinitesimal neighborhood of point $\gamma^{(X)}(Y)|_{Y=X}$, which is stress-free. Synthesize upon the family $(\boldsymbol{F}^{(X)})_{X\in\mathbb{S}_I}$ the new field $\boldsymbol{H}$ of linear mappings as follows:

$$\boldsymbol{H} : \mathbb{S}_I \to \mathrm{Lin}(\mathbb{V}; \mathbb{V}), \quad X \mapsto \boldsymbol{H}_X := \boldsymbol{F}^{(X)}_Y|_{Y=X}. \tag{5.4}$$

According to definition, for each $X \in \mathbb{S}_I$ the linear map $\boldsymbol{H}_X$ transforms infinitesimal neighborhood of X to stress-free state. We refer to the field $\boldsymbol{H}$ as field of local deformations. Since it is synthesized upon distinct deformation gradients, it is not the gradient of some map $\xi : \mathbb{S}_I \to \mathbb{E}$ that globally relaxes shape $\mathbb{S}_I$ to stress-free state.

Within our considerations, the Lagrangian density (5.1) of conventional elasticity should be modified to the form

$$\mathscr{L} = \mathscr{L}(X, t, \gamma, \boldsymbol{\nabla}\gamma, \dot{\gamma}, \boldsymbol{H}, \dot{\boldsymbol{H}}).$$

Here $\gamma : \mathbb{S}_I \times [t_0, t_1] \to \mathbb{E}$ and $\boldsymbol{H} : \mathbb{S}_I \times [t_0, t_1] \to \mathrm{Lin}(\mathbb{V}; \mathbb{V})$ are, respectively, the motion of the shape $\mathbb{S}_I$ and time-dependent field of local deformations. Both are considered as independent field quantities.

20°. Principle of local discharging: micromorphic kinematics. For definiteness, suppose that we deal with enhanced physical space and shapes which are modeled as vector bundles. Then enhanced deformation between two shapes is represented by formula (5.10) from Appendix, while micromorphic deformation is represented by formula (3.5):

$$V\gamma(X) = (\gamma(X), \boldsymbol{\mathcal{M}}(X)[U_X]),$$

where γ is conventional deformation and $\boldsymbol{\mathcal{M}}(X) \in \mathrm{Lin}(\mathbb{F}; \mathbb{F})$ is linear map, which relates reference and actual directors. In this case the principle of local discharging is assumed to be of the form: there exist a shape $\mathbb{S}_I$ in physical space $\mathbb{E}$, a family $(\gamma^{(X)})_{X\in\mathbb{S}_I}$ of deformations $\gamma^{(X)} : \mathbb{S}_I \to \mathbb{S}^{(X)}$ from the shape $\mathbb{S}_I \subset \mathbb{E}$ to some shapes $\mathbb{S}^{(X)}$ and a family $(\boldsymbol{\mathcal{M}}^{(X)})_{X\in\mathbb{S}_I}$ of directors $\boldsymbol{\mathcal{M}}^{(X)} : \mathbb{S}_I \to \mathrm{Lin}(\mathbb{F}; \mathbb{F})$, such that the infinitesimal neighborhood of point $V\gamma^{(X)}(Y)|_{Y=X} = (\gamma^{(X)}(Y)|_{Y=X}, \boldsymbol{\mathcal{M}}^{(X)}(Y)|_{Y=X})$ is stress-free for any $X \in \mathbb{S}_I$.

We utilize the procedure of synthesizing to deformation gradients $\boldsymbol{F}^{(X)} = \boldsymbol{\nabla}\gamma : \mathbb{S}_I \to \mathrm{Lin}(\mathbb{V}; \mathbb{V})$, and to director gradients $\boldsymbol{\nabla}\boldsymbol{\mathcal{M}}^{(X)} : \mathbb{S}_I \to \mathrm{Lin}(\mathbb{V}; \mathrm{Lin}(\mathbb{F}; \mathbb{F}))$. This results in field (5.4) of local deformations (like in the case of simple solid), and in field

$$\boldsymbol{D} : \mathbb{S}_I \to \mathrm{Lin}(\mathbb{V}; \mathrm{Lin}(\mathbb{F}; \mathbb{F})), \quad X \mapsto \boldsymbol{D}_X = \boldsymbol{\nabla}_Y \boldsymbol{\mathcal{M}}^{(X)}|_{Y=X},$$

synthesized upon gradients of microdeformation tensors.

In the case of micromorphic kinematics the Lagrangian density (4.6) of micromorphic elasticity is modified to the form

$$\mathscr{L} = \mathscr{L}(X,\, t,\, \gamma,\, \boldsymbol{\nabla}\gamma,\, \dot{\gamma},\, \boldsymbol{\mathcal{M}},\, \boldsymbol{\nabla}\boldsymbol{\mathcal{M}},\, \dot{\boldsymbol{\mathcal{M}}},\, \boldsymbol{H},\, \dot{\boldsymbol{H}},\, \boldsymbol{D},\, \boldsymbol{\nabla}\boldsymbol{D},\, \dot{\boldsymbol{D}}).$$

Here $\gamma : \mathbb{S}_I \times [t_0,\, t_1] \to \mathbb{E}$, $\boldsymbol{\mathcal{M}} : \mathbb{S}_I \times [t_0,\, t_1] \to \mathrm{Lin}(\mathbb{F};\, \mathbb{F})$ and $\boldsymbol{H} : \mathbb{S}_I \times [t_0,\, t_1] \to \mathrm{Lin}(\mathbb{V};\, \mathbb{V})$, $\boldsymbol{D} : \mathbb{S}_I \times \times [t_0,\, t_1] \to \mathrm{Lin}(\mathbb{V};\, \mathrm{Lin}(\mathbb{F};\, \mathbb{F}))$ are, respectively, the motion of the shape $\mathbb{S}_I$ and time-dependent fields of local deformations. Maps γ, $\boldsymbol{\mathcal{M}}$, $\boldsymbol{H}$, and $\boldsymbol{D}$ are considered as independent field quantities.

5.2. Geometrical Viewpoint

21°. Simple body. Considerations of section 5.1. were based on the rejection of using the global stress-free shape. Instead of this, one deals with family of locally stress-free shapes. Meanwhile, the concept of global stress-free shape is attractive enough, since one can deal with material description of processes, which is commonly convenient in non-linear elasticity. To allow global stress-free shapes, one just needs to go beyond Euclidean structure and consider manifolds equipped with non-Euclidean geometry. Choosing appropriate geometry, one obtains global stress-free shape and then deformations become embeddings of non-Euclidean stress-free shape to Euclidean space.

The stress-free shape is modeled on the intermediate shape $\mathbb{S}_I = (S_I,\, \mathcal{T}_E|_{S_I},\, \mathcal{D}_E|_{S_I},\, \boldsymbol{g}_E|_{S_I},\, \nabla_E|_{S_I})$. To do this, one needs to erase Euclidean structure from it. Thus results in manifold $M_R = (S_I,\, \mathcal{T}_E|_{S_I},\, \mathcal{D}_E|_{S_I})$, pure from any geometry. Let $\boldsymbol{H} : M_I \to \mathrm{Lin}(\mathbb{V};\, \mathbb{V})$ be field of local deformations. One can use it to introduce geometry on M_I.

Riemannian metric $\mathsf{G} : M_I \to T^*M_I \otimes T^*M_I$ is defined on M_I upon field of local deformations as follows:

$$\mathsf{G}_X(\mathsf{u},\, \mathsf{v}) := \boldsymbol{H}_X[\mathsf{u}] \cdot \boldsymbol{H}_X[\mathsf{u}], \tag{5.5}$$

for all $X \in M_I$ and $\mathsf{u}, \mathsf{v} \in T_X M_I$. Let us explain the action of "Euclidean" tensor $\boldsymbol{H}_X \in \mathrm{Lin}(\mathbb{V}; \mathbb{V})$ on abstract tangent vector from $T_X M_I$. Since we consider the case $\dim \mathfrak{B} = 3$, the shape M_I is open submanifold of $\mathbb{E}$. Then there is natural vector space isomorphism $T_X M_I \cong \mathbb{V}$ [25]. By this reason, we tacitly identify element of $\mathrm{Lin}(\mathbb{V};\, \mathbb{V})$ with element of $\mathrm{Lin}(T_X M_I;\, \mathbb{V})$.

The value G_X of field G is non-degenerate symmetric positive-definite bilinear form on $T_X M_I$, that defines metric structure on $T_X M_I$. Upon tangent vectors $\mathsf{u}, \mathsf{v} \in T_X M_I$, which are infinitesimal material fibers, it returns the inner product $\boldsymbol{u} \cdot \boldsymbol{v}$ of their relaxed images $\boldsymbol{u} = \boldsymbol{H}_X[\mathsf{u}]$ and $\boldsymbol{v} = \boldsymbol{H}_X[\mathsf{v}]$. Thus, one obtains lengths of material fibers and angles between them as if they where in relaxed state.

There are several possibilities to introduce affine connection ∇ on M_I [26, 36]. One of them, the Weitzenböck connection, is chosen in the study. Its connection functions in coordinate frame are given by relations

$$\Gamma^i{}_{jk} = -\boldsymbol{H}^c{}_k \partial_{X^j} [\boldsymbol{H}^{-1}]^i{}_c = [\boldsymbol{H}^{-1}]^i{}_c \partial_{X^j} \boldsymbol{H}^c{}_k, \tag{5.6}$$

where $\boldsymbol{H}^{-1} : X \mapsto \boldsymbol{H}_X^{-1}$ is field of inverse local deformations. The deviation of this connection from Euclidean one is completely characterized by torsion tensor field $\mathfrak{T}$. Thus, $\mathfrak{T}$ may serve as the measure of inhomogeneity.

Thus, one arrives at non-Euclidean space $\mathcal{S} = (M_I,\, \mathsf{G},\, \nabla)$, to which we refer as *non-Euclidean reference shape*. Any deformation is then an embedding $\lambda : \mathcal{S} \to \mathbb{E}$ of non-Euclidean manifold into Euclidean one. It can be decomposed into two deformations,

$$\lambda = \gamma \circ \psi,$$

where $\psi : \mathcal{S} \to \mathbb{S}_I$ is a smooth map that "imprints" non-Euclidean shape into Euclidean space. More formally, it replaces the structure $(M_I, \mathsf{G}, \nabla)$ with underlying manifold M_I by the structure[17] $(M_I, \boldsymbol{g}_E|_{S_I}, \nabla_E|_{S_I})$ with the same underlying manifold M_I, such that $X \mapsto X$. Other map $\gamma : \mathbb{S}_I \to \mathbb{E}$ is conventional deformation between Euclidean shapes.

Since $\mathcal{S}$ is manifold with non-Euclidean parallel transport rule, one cannot use Euclidean differentiation operator $\boldsymbol{\nabla}$. Instead of it, one can use tangent map operation T [25]. Being applied to deformation λ, it results in the map $T\lambda : T\mathcal{S} \to T\mathbb{E}$, which can be considered as the collection of linear maps $T_X\lambda : T_X\mathcal{S} \to T_{\lambda(X)}\mathbb{E}$, $X \in \mathcal{S}$, with matrices $[T\lambda]$ in coordinate frame defined as follows:

$$[T\lambda] = D(\varphi \circ \lambda \circ \sigma^{-1}),$$

where $\sigma : \mathcal{S} \to \mathbb{R}^3$ is coordinate map on $\mathcal{S}$ and $\varphi : \mathbb{E} \to \mathbb{R}^3$ is coordinate map on $\mathbb{E}$. The symbol D stands for total derivative in $\mathbb{R}^3$.

Assuming all considered fields as time-dependent, one can introduce the following Lagrangian density:

$$\mathscr{L} = \mathscr{L}(X,\, t,\, \lambda,\, T\lambda,\, \dot{\lambda},\, \mathsf{G},\, \dot{\mathsf{G}},\, \mathfrak{T},\, \dot{\mathfrak{T}}). \tag{5.7}$$

[17] Here $\boldsymbol{g}_E$ is metric tensor on $\mathbb{E}$.

Here X is point on the shape $\mathcal{S}$, $\lambda : \mathcal{S} \times [t_0, t_1] \to \mathbb{E}$ is a motion, and G, $\mathfrak{T}$ are, respectively, time-dependent metric and torsion.

22°. Micromorphic body. The case of micromorphic continuum can be considered in a similar manner. One starts with some submanifold $VM_I \subset V\mathbb{E}$, the substructure of intermediate shape $V\mathbb{S}_I$, pure from any geometry. Meanwhile, in contrast to the previous considerations, one has two tensor fields of local deformations: $\boldsymbol{H} : M_I \to \mathrm{Lin}(\mathbb{V}; \mathbb{V})$ and $\boldsymbol{D} : M_I \to \mathrm{Lin}(\mathbb{V}; \mathrm{Lin}(\mathbb{F}; \mathbb{F}))$. Here M_I is the base manifold. Moreover, we suppose that model fiber $\mathbb{F}$ has inner product structure, which, in turn, induces inner product $(:)$ on $\mathrm{Lin}(\mathbb{F}; \mathbb{F})$.

Using natural isomorphism $T_X M_I \cong \mathbb{V}$, we define two Riemannian metrics on M_I. One is the Riemannian metric G, introduced by formula (5.5). The second field $\mathsf{G}^{\mathbb{F}} : M_I \to T^*M_I \otimes T^*M_I$ is defined by the following equality:

$$\mathsf{G}^{\mathbb{F}}_X[\mathsf{u}, \mathsf{v}] = \boldsymbol{D}_X[\mathsf{u}] : \boldsymbol{D}_X[\mathsf{v}], \tag{5.8}$$

for all $X \in M_I$ and $\mathsf{u}, \mathsf{v} \in T_X M_I$. The metric $\mathsf{G}^{\mathbb{F}}$ is a metric over orientations, i. e., with each point $X \in M_I$ it associates a machine, that measures lengths of orientations associated with point X and angles between them.

Similarly to metrics, we introduce two connections on M_I. One is affine connection ∇ on M_I with connection functions defined as (5.6). Its torsion tensor $\mathfrak{T}$ characterizes the inhomogeneity within particles. Using metric field $\mathsf{G}^{\mathbb{F}}$ defined by (5.8), one can induce Levi-Civita connection $\nabla^{\mathbb{F}}$ on M_I. Its curvature tensor $\mathfrak{R}^{\mathbb{F}}$ characterizes the inhomogeneity within micro-particles. Thus, instead of (5.7), one arrives at the following Lagrangian density:

$$\mathscr{L} = \mathscr{L}(X, t, \lambda, T\lambda, \dot{\lambda}, \mathsf{G}, \dot{\mathsf{G}}, \mathfrak{T}, \dot{\mathfrak{T}}, \mathsf{G}^{\mathbb{F}}, \dot{\mathsf{G}}^{\mathbb{F}}, \mathfrak{R}^{\mathbb{F}}, \dot{\mathfrak{R}}^{\mathbb{F}}), \tag{5.9}$$

where $X \in M_I$ and mapping $\lambda : M_I \times [t_0, t_1] \to \mathbb{E}$ corresponds to motion.

Conclusions

We point out the following positions of the classical method, which are specific for oriented solids and shell-like solids with incompatible deformations.

1. The action is formulated with respect to intermediate shape, which is related with the continuous family of local stress free shapes. This brings additional field arguments, namely implants (with translation and microdeformational character), to the Lagrangian density.

2. It is possible to formulate the action with respect to single stress-free shape, but, generally, this shape will be non-Euclidean.

3. The principal difference between models for micropolar, micromorphic and shell-like solids is encoded in the structure of bundles, that are used for enhanced manifold definition.

4. Most general structure that characterize embedding of smooth material bundle into smooth physical bundle is too wide for all conventional models, because it takes into account a continuum of possible orientations for each material point. Meanwhile one can derive from it conventional models for oriented solids and shells by constructing specific sections over the bundles.

Appendix

23°. Metric and connection on body manifold. Let us consider in more detail what gives the use of metric and connection in the structure of body manifold. Riemannian metric $\mathsf{g}_B : \mathfrak{B} \to T^*\mathfrak{B} \otimes T^*\mathfrak{B}$ satisfies the following defining properties at each point $\mathfrak{X} \in \mathfrak{B}$ [25]:

- for all tangent vectors $\mathsf{u}, \mathsf{v} \in T_{\mathfrak{X}}\mathfrak{B}$ one has that $\mathsf{g}_B|_{\mathfrak{X}}(\mathsf{u}, \mathsf{v}) = \mathsf{g}_B|_{\mathfrak{X}}(\mathsf{v}, \mathsf{u})$;

- for each vector $\mathsf{u} \in T_{\mathfrak{X}}\mathfrak{B}$, $\mathsf{g}_B|_{\mathfrak{X}}(\mathsf{u}, \mathsf{u}) \geqslant 0$;

- for any vector $\mathsf{u} \in T_{\mathfrak{X}}\mathfrak{B}$, $\mathsf{g}_B|_{\mathfrak{X}}(\mathsf{u}, \mathsf{u}) = 0$ iff $\mathsf{u} = \mathsf{0}$.

Thus, the bilinear form $(\mathsf{u}, \mathsf{v}) \mapsto \mathsf{g}_B|_{\mathfrak{X}}(\mathsf{u}, \mathsf{v})$ is an inner product on tangent space $T_{\mathfrak{X}}\mathfrak{B}$. One can measure lengths of tangent vectors and angles between them. After embedding $\varkappa : \mathfrak{B} \to \mathbb{E}$ to physical manifold one can compare metric information on $\mathfrak{B}$ with metric information on the image $\varkappa(\mathfrak{B})$ of the embedding. In the framework of conventional elasticity this description gives nothing new, since one deals not with body, but with some fixed privileged subspace of $\mathbb{E}$, shape of the body. Usually it is assumed that this shape is stress-free.

Meanwhile, for solid with defects one cannot find such the shape in Euclidean physical space. Geometric methodology, developed in the papers [22; 23; 36–38] suggests to fix the issue by using non-Euclidean shapes, modeled on the body manifold. Then metric g_B acquires the certain sense: it gives reference (in stress-free state) lengths and angles of infinitesimal material fibers, formalized as tangent vectors. At the same time, one needs an extra information: to formulate balance equations on the body manifold one needs certain parallel transport rule. This rule can be established be means of the affine connection ∇_B, which to any pair (u, v) of vector fields on $\mathfrak{B}$ assigns vector field $(\nabla_B)_{\mathsf{u}}\mathsf{v}$ on the same body manifold. The following requirements are satisfied [39]:

- $(\nabla_B)_{\mathsf{u}+\mathsf{v}}\mathsf{w} = (\nabla_B)_{\mathsf{u}}\mathsf{w} + (\nabla_B)_{\mathsf{v}}\mathsf{w}$,
- $(\nabla_B)_{f\mathsf{u}}\mathsf{v} = f(\nabla_B)_{\mathsf{u}}\mathsf{v}$,
- $(\nabla_B)_{\mathsf{u}}(\mathsf{v}+\mathsf{w}) = (\nabla_B)_{\mathsf{u}}\mathsf{v} + (\nabla_B)_{\mathsf{u}}\mathsf{w}$,
- $(\nabla_B)_{\mathsf{u}}(f\mathsf{v}) = f(\nabla_B)_{\mathsf{u}}\mathsf{v} + (\mathsf{u}f)\mathsf{v}$,

for vector fields u, v, $\mathsf{w} : \mathfrak{B} \to T\mathfrak{B}$ and scalar function $f : \mathfrak{B} \to \mathbb{R}$. Affine connection endows body with some geometry. Each geometry is characterized by tensor fields of torsion $\mathfrak{T}$, curvature $\mathfrak{R}$ and nonmetricity $\mathfrak{Q}$ [24]. The correspondence to each space is shown on Table 2, where the symbol $\circ$ illustrates that the corresponding field vanishes, while $\bullet$ designates that field takes nonzero values.

Table 2

Correspondence between geometries and tensor fields of torsion, curvature and nonmetricity

Geometry	Torsion ($\mathfrak{T}$)	Curvature ($\mathfrak{R}$)	Nonmetricity ($\mathfrak{Q}$)
Riemann	$\circ$	$\bullet$	$\circ$
Weitzenböck	$\bullet$	$\circ$	$\circ$
Weyl	$\circ$	$\circ$	$\bullet$

24°. Enhanced kinematics for vector bundles. The mapping ε from (3.3) has general form in the case of arbitrary fiber bundles. Meanwhile, vector bundle and principal bundle structures induce some particular properties of ε. Consider the case of vector bundle first. Physical bundle is represented by structure $(V\mathbb{E}, \mathbb{E}, \pi_{\mathbb{E}}, \mathbb{F})$, which is vector bundle of rank m, like material bundle. The enhanced configuration $V\varkappa : V\mathfrak{B} \to V\mathbb{E}$ and enhanced deformation $V\gamma : V\mathbb{S}_R \to V\mathbb{S}$ are related to conventional configuration $\varkappa : \mathfrak{B} \to \mathbb{E}$ and conventional deformation $\gamma : \mathbb{S}_R \to \mathbb{S}$ according to the general formulae (3.1) and (3.2):

$$\varkappa \circ \pi_{\mathfrak{B}} = \pi_{\mathbb{E}} \circ V\varkappa, \quad \gamma \circ \pi_{\mathbb{E}} = \pi_{\mathbb{E}} \circ V\gamma.$$

Moreover, it is required that mappings $V\varkappa$ and $V\gamma$ are compatible with vectorial structure of the bundle[18] [25]: for any $\mathfrak{X} \in \mathfrak{B}$ the restriction $V\varkappa|_{V\mathfrak{B}_{\mathfrak{X}}} : V\mathfrak{B}_{\mathfrak{X}} \to V\mathbb{E}_{\varkappa(\mathfrak{X})}$ to fibers of $V\mathfrak{B}$ is linear map, and for any $X \in \mathbb{S}_R$ the restriction[19] $V\gamma|_{V\mathbb{S}_{R;\,X}} : V\mathbb{S}_{R;\,X} \to V\mathbb{S}_{\gamma(X)}$ to fibers of $V\mathbb{S}_R$ is also a linear map.

Introduce natural coordinates $(X^1, ..., X^n; U^1, ..., U^m)$ on the enhanced reference shape $V\mathbb{S}_R$ and natural coordinates $(x^1, ..., x^n; u^1, ..., u^m)$ on the enhanced actual shape $V\mathbb{S}$. Let $\tilde{\gamma} : (X^1, ..., X^n) \mapsto (x^1, ..., x^n)$ be coordinate representation of conventional deformation γ. Then bundle structure gives the following equality for coordinate representation $\widetilde{V\gamma} : \mathbb{R}^{m+n} \to \mathbb{R}^{m+n}$ of $V\gamma$:

$$\widetilde{V\gamma}(X^1, ..., X^n; U^1, ..., U^m) = (\tilde{\gamma}(X^1, ..., X^n); \tilde{\boldsymbol{\mathcal{M}}}(X^1, ..., X^3; U^1, ..., U^m)),$$

where $\tilde{\boldsymbol{\mathcal{M}}} : \mathbb{R}^{m+n} \to \mathbb{R}^m$ gives coordinate representation of actual orientations. The linearity condition imposed on enhanced deformation imply that partial map $\tilde{\boldsymbol{\mathcal{M}}}(X^1, ..., X^n, \cdot) : \mathbb{R}^m \to \mathbb{R}^m$ is linear.

Consider particular case, when physical vector bundle is trivial, i. e., $V\mathbb{E}$ is diffeomorphic to product space $\mathbb{E} \times \mathbb{F}$ via local trivialization Φ. Then, since vector bundle structures are trivial, the enhanced deformation is the mapping $V\gamma : \mathbb{S}_R \times \mathbb{F} \to \mathbb{S} \times \mathbb{F}$, which values are of the form

$$(x, u) = V\gamma(X, U) = (\gamma(X), \boldsymbol{\mathcal{M}}(X, U)), \tag{5.10}$$

where assignment $\boldsymbol{\mathcal{M}} : \mathbb{S}_R \times \mathbb{F} \to \mathbb{F}$ returns actual orientations and it is such that its partial map $\boldsymbol{\mathcal{M}}(X, \cdot\,\cdot) : \mathbb{F} \to \mathbb{F}$, $\boldsymbol{\mathcal{M}}(X, \cdot) : U \mapsto \boldsymbol{\mathcal{M}}(X, U)$ is linear. Thus, in the case of trivial vector bundle we obtain that deformation of solid with extra degrees of freedom is characterized by conventional deformation $\gamma : \mathbb{S}_R \to \mathbb{S}$ and so-called microdeformation tensor $\boldsymbol{\mathcal{M}} : \mathbb{S}_R \times \mathbb{F} \to \mathbb{F}$.

[18] If not so, we won't obtain "nice" properties of the map ε.

[19] Here, as in general case of fiber bundle, we induce vector bundle structures on shapes: $(V\mathbb{S}_R, \mathbb{S}_R, \pi_{\mathbb{E}}|_{V\mathbb{S}_R}, \mathbb{F})$, and $(V\mathbb{S}, \mathbb{S}, \pi_{\mathbb{E}}|_{V\mathbb{S}}, \mathbb{F})$.

25°. Enhanced kinematics for principal bundles. Finally, we equip physical space $\mathbb{E}$ with principal bundle structure $(P\mathbb{E}, \mathbb{E}, \pi_{\mathbb{E}}, G, \top, \lhd_{\mathbb{E}})$, which structure group G is similar to the structure group of material principal bundle $(P\mathfrak{B}, \mathfrak{B}, \pi_{\mathfrak{B}}, G, \top, \lhd_{\mathfrak{B}})$. For further reasonings it would be convenient to denote coordinate tuples on base and structure group by putting tilde above. In particular, $\widetilde{\mathfrak{X}} = (\mathfrak{X}^1, ..., \mathfrak{X}^n)$ and $\widetilde{\mathfrak{g}} = (\mathfrak{g}^1, ..., \mathfrak{g}^m)$.

By enhanced configuration of enhanced body $P\mathfrak{B}$ to enhanced physical space $P\mathbb{E}$ we mean a smooth mapping $P\varkappa : P\mathfrak{B} \to P\mathbb{E}$, that satisfies the equivariance condition [29]:

$$\forall p \in P\mathfrak{B}\, \forall g \in G : \; P\varkappa(p \lhd_{\mathfrak{B}} g) = P\varkappa(p) \lhd_{\mathbb{E}} g. \tag{5.11}$$

In other words, $P\varkappa$ preserves principal bundle structure. In particular, it preserves layers and by this reason it induces embedding $\varkappa : \mathfrak{B} \to \mathbb{E}$, conventional configuration, such that the equality (3.1) holds.

Relation (3.1) induces representation of enhanced configuration $P\varkappa$ in natural coordinates:

$$\widetilde{P\varkappa}(\widetilde{\mathfrak{X}};\, \widetilde{\mathfrak{g}}) = (\widetilde{\varkappa}(\widetilde{\mathfrak{X}});\, \widetilde{\tau}(\widetilde{\mathfrak{X}};\, \widetilde{\mathfrak{g}})),$$

where $\widetilde{\varkappa} : \widetilde{\mathfrak{X}} \mapsto \widetilde{x}$ is coordinate representation of conventional configuration $\varkappa$, while $\widetilde{\tau} : (\widetilde{\mathfrak{X}}; \widetilde{\mathfrak{g}}) \mapsto \widetilde{\mathfrak{g}}$ corresponds to configuration of orientations. Moreover, equivariance condition (5.11) gives

$$\tau(\widetilde{p} \widetilde{\lhd}_{\mathfrak{B}} \widetilde{h}) = \tau(\widetilde{p}) \widetilde{\top} \widetilde{h}.$$

Let $P\varkappa_R$, $P\varkappa : P\mathfrak{B} \to P\mathbb{E}$ be enhanced configurations of enhanced body $P\mathfrak{B}$, and let $\varkappa_R$, $\varkappa : \mathfrak{B} \to \mathbb{E}$ be corresponding conventional configurations of the body manifold $\mathfrak{B}$. Then images $P\mathbb{S}_R = P\varkappa_R(P\mathfrak{B})$ and $P\mathbb{S} = P\varkappa(P\mathfrak{B})$ correspond to enhanced shapes of $P\mathfrak{B}$ in enhanced physical space $P\mathbb{E}$. The composition $P\gamma = \widehat{P\varkappa} \circ \widehat{P\varkappa_R}^{-1} : P\mathbb{S}_R \to P\mathbb{S}$ of enhanced configurations correspond to enhanced deformation in enhanced physical space $P\mathbb{E}$, while $\gamma = \widehat{\varkappa} \circ \widehat{\varkappa}_R^{-1} : \mathbb{S}_R \to \mathbb{S}$ is conventional deformation of reference set of places $\mathbb{S}_R$ to the actual one, $\mathbb{S}$.

In natural coordinates on enhanced shapes the coordinate representation of enhanced deformation has the form

$$\widetilde{P\gamma}(\widetilde{X};\, \widetilde{G}) = (\widetilde{\gamma}(\widetilde{X});\, \widetilde{\varepsilon}(\widetilde{X};\, \widetilde{G})).$$

Here $\widetilde{\gamma} : \widetilde{X} \mapsto \widetilde{x}$ is coordinate representation of γ, while $\widetilde{\varepsilon} : (\widetilde{X};\, \widetilde{X}) \mapsto \widetilde{g}$ returns actual orientations.

It can be shown that $P\gamma$ is equivariant, i. e., it satisfies the property similar to (3.1). Then the mapping $\widetilde{\varepsilon}$ has the "homogeneity" property with respect to elements of G:

$$\widetilde{\varepsilon}(\widetilde{X};\, \widetilde{G} \widetilde{\top} \widetilde{H}) = \widetilde{\varepsilon}(\widetilde{X};\, \widetilde{G}) \widetilde{\top} \widetilde{H}.$$

Suppose that G can be covered by one chart. Then, if set $\Psi(\widetilde{X}) := \widetilde{\varepsilon}(\widetilde{X};\, \widetilde{1})$, where $\widetilde{1}$ is coordinate representation of identity of G, one obtains $\widetilde{\varepsilon}(\widetilde{X};\, \widetilde{G}) = \Psi(\widetilde{X}) \widetilde{\top} \widetilde{G}$, that gives

$$\widetilde{P\gamma}(\widetilde{X};\, \widetilde{G}) = (\widetilde{\gamma}(\widetilde{X});\, \Psi(\widetilde{X}) \widetilde{\top} \widetilde{G}).$$

Supposing that physical principal bundle is trivial[20], i. e., $P\mathbb{E} = \mathbb{E} \times G$, one obtains that enhanced deformation $P\gamma : \mathbb{S}_R \times G \to \mathbb{S} \times G$ can be expressed in the form

$$P\gamma(X,\, g) = (\gamma(X),\, \varepsilon(X,\, g)),$$

where $\gamma : \mathbb{S}_R \to \mathbb{S}$ is conventional deformation, and $\varepsilon : \mathbb{S}_R \times G \to G$ returns actual orientations. If we put $\Psi(X) := \varepsilon(X,\, 1)$, where 1 is the identity of G, then, since $\varepsilon(X,\, g) = \Psi(X) \top g$, one gets

$$P\gamma(X,\, g) = (\gamma(X),\, \Psi(X) \top g).$$

Thus, deformation of oriented solid is characterized by mappings $\gamma : \mathbb{S}_R \to \mathbb{S}$ and $\Psi : \mathbb{S}_R \to G$.

References

[1] Lebedev L.P., Cloud M.J., Eremeyev V.A. Tensor Analysis with Applications in Mechanics. World Scientific, 2010. DOI: https://doi.org/10.1142/7826.

[2] Ciarlet P.G. Mathematical elasticity. Volume II, Theory of Plates. Elsevier, 1997. DOI: https://doi.org/10.1016/s0168-2024%2897%29x8001-4.

[3] Ciarlet P.G.: Mathematical elasticity. Volume III, Theory of Shells. North Holland, 2000, 659 p. Available at: https://readli.net/theory-of-shells/.

[4] Libai A., Simmonds J.G. The Nonlinear Theory of Elastic Shells. Cambridge: Cambridge University Press, 1998. DOI: https://doi.org/10.1017/CBO9780511574511.

[20] Then action of Lie group is defined as $(x,\, g) \lhd_{\mathbb{E}} h := (x,\, g \top h)$.

[5] Ambartsumian S.A. Micropolar Theory of Shells and Plates. Erevan: Nats. akad. nauk Resp. Armeniya. In-t problem informatiki i avtomatizatsii. Lab. komp'yuter. poligrafii, 1999. (In Russ.)

[6] Eremeyev V.A., Altenbach H. Basics of Mechanics of Micropolar Shells. In: Altenbach H., Eremeyev V.A. (eds.) Shell-like Structures. CISM International Centre for Mechanical Sciences (Courses and Lectures), vol. 572. Heidelberg: Springer, Cham, 2017, pp. 63–111. DOI: https://doi.org/10.1007/978-3-319-42277-0_2.

[7] Zubov L.M., Eremeyev V.A. Mechanics of elastic micropolar shells. *Far Eastern Mathematical Journal*, 2003, vol. 4, no. 2, pp. 182–225. Available at: http://mi.mathnet.ru/dvmg158. (In Russ.)

[8] Zhilin P.A. Basic equations of non-classical theory of elastic shells. *Dinamika i prochnost' mashin: Trudy Leningradskogo politekhnicheskogo instituta*, 1982, vol. 386, pp. 29–46. (In Russ.)

[9] Wang C.C. Universal Solutions for Incompressible Laminated Bodies. In: Noll W., Toupin R.A., Wang C.C. *Continuum Theory of Inhomogeneities in Simple Bodies.* Heidelberg: Springer, Cham, 1968, pp. 149–180. DOI: https://doi.org/10.1007/978-3-642-85992-2_6.

[10] Cohen H., Wang C.C. Some equilibrium problems for fibrillar bodies. *Archive for Rational Mechanics and Analysis*, 1993, vol. 123, no. 4, pp 337–375. DOI: https://doi.org/10.1007/BF00375584.

[11] Noll W. Materially uniform simple bodies with inhomogeneities. *Archive for Rational Mechanics and Analysis*, 1967, vol. 27, no. 1, pp. 1–32. DOI: https://doi.org/10.1007/BF00276433.

[12] Lewicka M., Mahadevan L., Pakzad M.R. Models for elastic shells with incompatible strains. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 2014, vol. 470, issue 2165. DOI: https://doi.org/10.1098/rspa.2013.0604.

[13] Lychev S.A. Equilibrium equations for transversely accreted shells. *ZAMM — Journal of Applied Mathematics and Mechanics. Zeitschrift fur Angewandte Mathematik und Mechanik*, 2014, vol. 94, no. 1-2, pp. 118–129. DOI: https://doi.org/10.1002/zamm.201200231.

[14] Lychev S.A., Altenbach H. Growing Solids and Thin-Walled Structures. *Procedia IUTAM*, 2017, vol. 23, pp. 13–32. DOI: https://doi.org/10.1016/j.piutam.2017.06.002.

[15] Epstein M., Leon M. Geometrical theory of uniform Cosserat media. *Journal of Geometry and Physics*, 1998, vol. 26, issue 1–2, pp. 127–170. DOI: https://doi.org/10.1016/S0393-0440(97)00042-9.

[16] Bucataru I., Epstein M. Geometrical theory of dislocations in bodies with microstructure. *Journal of Geometry and Physics*, 2004, vol. 52, no. 1, pp. 57–73. DOI: https://doi.org/10.1016/j.geomphys.2004.01.006.

[17] Postnikov M.M. Lectures in Geometry: Analytic Geometry. Moscow: URSS, 1994. Available at: http://alexandr4784.narod.ru/pmmgeo1.html. (In Russ.)

[18] Postnikov M.M.: Lectures in Geometry: Linear Algebra and Differential Geometry. URSS, 1994. Available at: http://alexandr4784.narod.ru/pmmgeo2.html. (In Russ.)

[19] Rudolph G., Schmidt M. Differential Geometry and Mathematical Physics. Part I. Manifolds, Lie Groups and Hamiltonian Systems. Springer Science+ Business Media Dordrecht, 2013. DOI: http://dx.doi.org/10.1007/978-94-007-5345-7.

[20] Rudolph G., Schmidt M. Differential Geometry and Mathematical Physics. Part II. Fibre Bundles, Topology and Gauge Fields. Springer Science+ Business Media Dordrecht, 2017. DOI: https://doi.org/10.1007/978-94-024-0959-8.

[21] Wang C.C. On the geometric structure of simple bodies, a mathematical foundation for the theory of continuous distributions of dislocations. In: Noll W., Toupin R.A., Wang C.C. *Continuum Theory of Inhomogeneities in Simple Bodies.* Springer, Heidelberg, 1968, pp. 87–148. DOI: https://doi.org/10.1007/978-3-642-85992-2_5.

[22] Yavari A., Goriely A. Riemann — Cartan geometry of nonlinear dislocation mechanics. *Archive for Rational Mechanics and Analysis*, 2012, vol. 205, no. 1, pp. 59–118. DOI: https://doi.org/10.1007/s00205-012-0500-0.

[23] Yavari A., Goriely A. Weyl geometry and the nonlinear mechanics of distributed point defects. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 2012, vol. 468, no. 2148, pp. 3902–3922. DOI: https://doi.org/10.1098/rspa.2012.0342.

[24] Lychev S.A., Koifman K.G. Geometry of Incompatible Deformations: Differential Geometry in Continuum Mechanics. De Gruyter, 2018. DOI: http://dx.doi.org/10.1515/9783110563214.

[25] Lee J.M. Introduction to Smooth Manifolds. New York: Springer, 2012. 486 p. Available at: http://inis.jinr.ru/sl/M_Mathematics/MD_Geometry%20and%20topology/MDdg_Differential%20geometry/Lee%20J.M.%20Introduction%20to%20smooth%20manifolds%20(draft,%202000)(486s).pdf.

[26] Lychev S.A., Koifman K.G. Material Affine Connections for Growing Solids. *Lobachevskii Journal of Mathematics*, 2020, vol. 41, no. 10, pp. 2034–2052. DOI: https://doi.org/10.1134/S1995080220100121.

[27] Husemoller D. Fibre Bundles. New York: Springer, 1994. Available at: https://www.maths.ed.ac.uk/ v1ranick/ papers/husemoller.

[28] Epstein M. Differential Geometry: Basic Notions and Physical Examples. Springer International Publishing, 2014. DOI: https://doi.org/10.1007/978-3-319-06920-3

[29] Naber G.L. Topology, Geometry and Gauge fields: Foundations. New York: Springer-Verlag, 2011. DOI: https://doi.org/10.1007/978-1-4419-7254-5

[30] Gurtin M.E., Murdoch A.I. A continuum theory of elastic material surfaces. *Archive for Rational Mechanics and Analysis*, 1975, vol. 57, no. 4, pp. 291–323. DOI: https://doi.org/10.1007/BF00261375.

[31] Marsden J.E., Hughes T.J. Mathematical foundations of elasticity. New York: Courier Corporation, 1994. Available at: https://resolver.caltech.edu/CaltechBOOK:1983.002.

[32] Lurie A.I. Analytical Mechanics. Moscow: GIFML, 1961. Available at: https://bookree.org/reader?file=450294&pg=1.

[33] Liang K.K. Efficient conversion from rotating matrix to rotation axis and angle by extending Rodrigues' formula. *arXiv*, 2018. Available at: https://arxiv.org/pdf/1810.02999.pdf.

[34] Delphenich D.H.: Mechanics of Cosserat media: I. non-relativistic statics. *arXiv*, 2012. Available at: https://arxiv.org/ftp/arxiv/papers/1212/1212.0399.pdf.

[35] Mindlin R.D. Micro-structure in linear elasticity. *Archive for Rational Mechanics and Analysis*, 1964, vol. 16, pp. 51–78. DOI: https://doi.org/10.1007/BF00248490.

[36] Lychev S.A., Koifman K.G. Contorsion of Material Connection in Growing Solids. *Lobachevskii Journal of Mathematics*, 2021, vol. 42, no. 8, pp. 1852–1875. DOI: https://doi.org/10.1134/S1995080221080187.

[37] Kupferman R., Olami E., Segev R. Continuum Dynamics on Manifolds: Application to Elasticity of Residually-Stressed Bodies. *Journal of Elasticity*, 2017, vol. 128, no. 1, pp. 61–84. DOI: http://doi.org/10.1007/s10659-016-9617-y.

[38] Lychev S.A, Kostin G.V., Koifman K.G., Lycheva T.N. Non-Euclidean Geometry and Defected Structure for Bodies with Variable Material Composition. *Journal of Physics: Conference Series*, 2019, vol. 1250, no. 1, p. 012035. DOI: http://doi:10.1088/1742-6596/1250/1/012035.

[39] Chern S.S., Chen W.H., Lam K.S. Lectures on Differential Geometry. World Scientific, 1999. DOI: https://doi.org/10.1142/3812.

Научная статья
DOI: 10.18287/2541-7525-2021-27-1-81-103

УДК 539.3

Дата: поступления статьи: 11.01.2021
после рецензирования: 15.02.2021
принятия статьи: 28.02.2021

С.А. Лычев
Институт проблем механики имени А.Ю. Ишлинского РАН,
г. Москва, Российская Федерация
E-mail: lychevsa@mail.ru. ORCID: https://orcid.org/0000-0001-7590-1389
К.Г. Койфман
Московский государственный технический университет
имени Н.Э. Баумана, г. Москва, Российская Федерация
E-mail: koifman.konstantin@gmail.com. ORCID: https://orcid.org/0000-0002-7891-9995
А.В. Дигилов
Институт проблем механики имени А.Ю. Ишлинского РАН,
г. Москва, Российская Федерация
E-mail: avdigilov@gmail.com. ORCID: https://orcid.org/0000-0001-6892-7740

НЕЛИНЕЙНЫЕ ДИНАМИЧЕСКИЕ УРАВНЕНИЯ ДЛЯ УПРУГИХ МИКРОМОРФНЫХ ТЕЛ И ОБОЛОЧЕК. ЧАСТЬ I[21]

АННОТАЦИЯ

В настоящей статье развивается общий подход к выводу нелинейных уравнений движения для деформируемых твердых тел, материальные точки которых обладают дополнительными степенями свободы. Характерной чертой этого подхода является учет несовместных деформаций, которые могут возникнуть в теле из-за распределенных дефектов или в результате некоторого процесса, например наращивания или ремоделирования. Математический формализм основан на принципе наименьшего действия и нетеровых симметриях. Особенность такого формализма заключается в формальном описании отсчетной конфигурации тела, которое в случае несовместных деформаций следует рассматривать или как непрерывное семейство

[21]Работа выполнена при поддержке государственной программы (контракт #АААА-А20-120011690132-4) и РФФИ (грант No. 18-29-03228).

форм, или как некоторую форму, вложенную в неевклидово пространство. Хотя общий подход дает уравнения для деформируемых твердых тел типа Коссера, микроморфных тел и оболочек, последние существенно отличаются по формальному описанию расширенной геометрической структуры, для которой необходимо определить интеграл действия. Это различие подробно обсуждается.

Ключевые слова: нелинейная динамика; микрополярные и микроморфные тела; оболочки; конечные деформации; несовместность деформаций; неевклидова отсчетная форма; расслоение; расширенные материальное и физическое многообразия; наименьшее действие; нетеровы симметрии; уравнения поля; законы сохранения.

Цитирование. Lychev S.A., Koifman K.G., Digilov A.V. Nonlinear dynamic equations for elastic micromorphic solids and shells. Part I // Вестник Самарского университета. Естественнонаучная серия. 2021. Т. 27, № 1. С. 81–103. DOI: http://doi.org/10.18287/2541-7525-2021-27-1-81-103.

Информация о конфликте интересов: авторы и рецензенты заявляют об отсутствии конфликта интересов.

© Лычев С.А., 2021
Сергей Александрович Лычев — доктор физико-математических наук, ведущий научный сотрудник, Институт проблем механики им. А.Ю. Ишлинского РАН, 119526, Российская Федерация, г. Москва, пр-кт Вернадского, 101, корп. 1.
© Койфман К.Г., 2021
Константин Георгиевич Койфман — ассистент, Московский государственный технический университет им. Н.Э. Баумана, 105005, Российская Федерация, г. Москва, 2-я Бауманская ул., 5.
© Дигилов А.В., 2021
Александр Вячеславович Дигилов — аспирант, Институт проблем механики им. А.Ю. Ишлинского РАН, 119526, Российская Федерация, г. Москва, пр-кт Вернадского, 101, корп. 1.

Литература

[1] Lebedev L.P., Cloud M.J., Eremeyev V.A. Tensor Analysis with Applications in Mechanics. World Scientific, 2010. DOI: https://doi.org/10.1142/7826.

[2] Ciarlet P.G. Mathematical elasticity. Volume II, Theory of Plates. Elsevier, 1997. DOI: https://doi.org/10.1016/s0168-2024 %2897%29x8001-4.

[3] Ciarlet P.G. Mathematical elasticity. Volume III, Theory of Shells. North Holland, 2000. Available at: https://readli.net/theory-of-shells/.

[4] Libai A., Simmonds J.G. The Nonlinear Theory of Elastic Shells. Cambridge: Cambridge University Press, 1998. DOI: https://doi.org/10.1017/CBO9780511574511.

[5] Амбарцумян С.А. Микрополярная теория оболочек и пластин. Ереван: Нац. акад. наук Респ. Армения. Ин-т проблем информатики и автоматизации. Лаб. компьютер. полиграфии, 1999.

[6] Eremeyev V.A., Altenbach H. Basics of Mechanics of Micropolar Shells // Altenbach H., Eremeyev V.A. (eds.) Shell-like Structures. CISM International Centre for Mechanical Sciences (Courses and Lectures), vol. 572. Heidelberg: Springer, Cham, 2017, pp. 63–111. DOI: https://doi.org/10.1007/978-3-319-42277-0_2.

[7] Зубов Л.М., Еремеев В.А. Механика упругих микрополярных оболочек // Дальневосточный математический журнал. 2003. Т. 4, № 2. С. 182–225. URL: http://mi.mathnet.ru/dvmg158.

[8] Жилин П.А. Основные уравнения неклассической теории оболочек. Труды Ленинградского политехнического института. 1982. № 386. С. 29–46.

[9] Wang C.C. Universal solutions for incompressible laminated bodies // Noll W., Toupin R.A., Wang C.C. Continuum Theory of Inhomogeneities in Simple Bodies. Springer, Heidelberg, 1968. P. 149–180. DOI: http://doi.org/10.1007/978-3-642-85992-2_6.

[10] Cohen H., Wang C.C. Some equilibrium problems for fibrillar bodies // Archive for Rational Mechanics and Analysis, 1993, vol. 123, no. 4, pp 337–375. DOI: http://doi.org/10.1007/BF00375584.

[11] Noll W. Materially uniform simple bodies with inhomogeneities // Archive for Rational Mechanics and Analysis, 1967, vol. 27, no. 1, pp. 1–32. DOI: http://doi.org/10.1007/BF00276433.

[12] Lewicka M., Mahadevan L., Pakzad M.R. Models for elastic shells with incompatible strains roceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 2014, vol. 470, no. 2165. DOI: http://doi.org/10.1098/rspa.2013.0604.

[13] Lychev S.A. Equilibrium equations for transversely accreted shells // ZAMM — Journal of Applied Mathematics and Mechanics. Zeitschrift fur Angewandte Mathematik und Mechanik, 2014, vol. 94, no. 1–2, pp. 118–129. DOI: http://doi.org/10.1002/zamm.201200231.

[14] Lychev S.A., Altenbach H. Growing Solids and Thin-Walled Structures // Procedia IUTAM, 2017, vol. 23, pp. 13–22. DOI: http://doi.org/10.1016/j.piutam.2017.06.002.

[15] Epstein M., de Leon M. Geometrical theory of uniform Cosserat media // Journal of Geometry and Physics, 1998, vol. 26, no. 1–2, pp. 127–170. DOI: http://doi.org/10.1016/S0393-0440(97)00042-9.

[16] Bucataru I., Epstein M. Geometrical theory of dislocations in bodies with microstructure // Journal of Geometry and Physics, 2004, vol. 52, no. 1, pp. 57–73. DOI: http://doi.org/10.1016/j.geomphys.2004.01.006.

[17] Постников М.М. Лекции по геометрии: Аналитическая геометрия. Москва: URSS, 2017. URL: http://alexandr4784.narod.ru/pmmgeo1.html.

[18] Постников М.М. Лекции по геометрии: Линейная алгебра. Москва: URSS, 2017. URL: http://alexandr4784.narod.ru/pmmgeo2.html.

[19] Rudolph G., Schmidt M. Differential Geometry and Mathematical Physics. Part I. Manifolds, Lie Groups and Hamiltonian Systems. Springer Science + Business Media Dordrecht, 2013. DOI: http://dx.doi.org/10.1007/978-94-007-5345-7.

[20] Rudolph G., Schmidt M. Differential Geometry and Mathematical Physics. Part II. Fibre Bundles, Topology and Gauge Fields. Springer Science + Business Media Dordrecht, 2017. DOI: https://doi.org/10.1007/978-94-024-0959-8.

[21] Wang C.C. On the geometric structure of simple bodies, a mathematical foundation for the theory of continuous distributions of dislocations // Noll W., Toupin R.A., Wang C.C. Continuum Theory of Inhomogeneities in Simple Bodies. Springer, Heidelberg, 1968. P. 88–148. DOI: https://doi.org/10.1007/978-3-642-85992-2_5.

[22] Yavari A., Goriely A. Riemann–Cartan geometry of nonlinear dislocation mechanics // Archive for Rational Mechanics and Analysis, 2012, vol. 205, no. 1, pp. 59–118. DOI: http://doi.org/10.1007/s00205-012-0500-0.

[23] Yavari A., Goriely A. Weyl geometry and the nonlinear mechanics of distributed point defects // Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 2012, vol. 468, no. 2148, pp. 3902–3922. DOI: http://doi.org/10.1098/rspa.2012.0342.

[24] Lychev S.A., Koifman K.G.: Geometry of Incompatible Deformations: Differential Geometry in Continuum Mechanics. De Gruyter, 2018. DOI: http://dx.doi.org/10.1515/9783110563214.

[25] Lee J.M. Introduction to Smooth Manifolds. Springer, New York, 2012. URL: http://inis.jinr.ru/sl/M_Mathematics/MD_Geometry%20and%20topology/MDdg_Differential%20geometry/Lee%20J.M.%20Introduction%20to%20smooth%20manifolds%20(draft,%202000)(486s).pdf.

[26] Lychev S.A., Koifman K.G. Material Affine Connections for Growing Solids // Lobachevskii Journal of Mathematics, 2020, vol. 41, no. 10, pp. 2034–2052. DOI: http://doi.org/10.1134/S1995080220100121.

[27] Husemoller D. Fibre Bundles. New York: Springer, 1994. URL: http://www.maths.ed.ac.uk/ v1ranick/papers/husemoller.

[28] Epstein M. Differential Geometry: Basic Notions and Physical Examples. Springer International Publishing, 2014. DOI: https://doi.org/10.1007/978-3-319-06920-3

[29] Naber G.L. Topology, Geometry and Gauge fields: Foundations. New York: Springer-Verlag, 2011. DOI: https://doi.org/10.1007/978-1-4419-7254-5

[30] Gurtin M.E., Murdoch A.I.: A continuum theory of elastic material surfaces // Archive for Rational Mechanics and Analysis, 1975, vol. 57, no. 4, pp. 291–323. DOI: http://doi.org/10.1007/BF00261375.

[31] Marsden J.E., Hughes T.J. Mathematical foundations of elasticity. Courier Corporation, 1994. URL: http://resolver.caltech.edu/CaltechBOOK:1983.002.

[32] Лурье А.И. Аналитическая механика. Москва: ГИФМЛ, 1961. URL: http://bookree.org/reader?file=450294&pg=1.

[33] Liang K.K. Efficient conversion from rotating matrix to rotation axis and angle by extending Rodrigues' formula // arXiv, 2018. URL: http://arxiv.org/pdf/1810.02999.pdf.

[34] Delphenich D.H. Mechanics of Cosserat media: I. non-relativistic statics // arXiv, 2012. URL: http://arxiv.org/ftp/arxiv/papers/1212/1212.0399.pdf.

[35] Mindlin R.D. Micro-structure in linear elasticity // Archive for Rational Mechanics and Analysis, 1964, vol. 16, pp. 51–78. DOI: http://doi.org/10.1007/BF00248490.

[36] Lychev S.A., Koifman K.G. Contorsion of Material Connection in Growing Solids // Lobachevskii Journal of Mathematics, 2021, vol. 42, no. 8, pp. 1852–1875. DOI: http://doi.org/10.1134/S1995080221080187.

[37] Kupferman R., Olami E., Segev R. Continuum Dynamics on Manifolds: Application to Elasticity of Residually-Stressed Bodies // Journal of Elasticity, 2017, vol. 128, no. 1, pp. 61–84. DOI: http://doi.org/10.1007/s10659-016-9617-y.

[38] Lychev S.A, Kostin G.V., Koifman K.G., Lycheva T.N. Non-Euclidean Geometry and Defected Structure for Bodies with Variable Material Composition // Journal of Physics: Conference Series, 2019, vol. 1250, no. 1, p. 012035. DOI: http://doi:10.1088/1742-6596/1250/1/012035.

[39] Chern S.S., Chen W.H., Lam K.S. Lectures on Differential Geometry. World Scientific, 1999. DOI: https://doi.org/10.1142/3812.

ФИЗИКА
PHYSICS

Научная статья
DOI: 10.18287/2541-7525-2021-27-1-104-110

УДК 629.7.05

Дата: поступления статьи: 07.01.2021
после рецензирования: 04.02.2021
принятия статьи: 28.02.2021

А.А. Кузнецова
Самарский национальный исследовательский университет
имени академика С.П. Королева, г. Самара, Российская Федерация
E-mail: malina-jun@yandex.ru. ORCID: https://orcid.org/0000-0002-3670-2499
В.А. Салеев
Самарский национальный исследовательский университет
имени академика С.П. Королева, г. Самара, Российская Федерация
E-mail: saleev@samsu.ru. ORCID: https://orcid.org/0000-0003-0505-5564

РОЖДЕНИЕ ИЗОЛИРОВАННЫХ ФОТОНОВ С БОЛЬШИМИ ПОПЕРЕЧНЫМИ ИМПУЛЬСАМИ НА БАК В РЕДЖЕВСКОМ ПРЕДЕЛЕ КХД

АННОТАЦИЯ

В статье рассматривается рождение прямых изолированных фотонов с большими поперечными импульсами на БАК при энергии $\sqrt{S} = 13$ ТэВ в подходе реджезации партонов, который основан на теореме факторизации жестких процессов при высоких энергиях и эффективной теории реджезованных глюонов и кварков Л.Н. Липатова. Неинтегрированные партонные распределения в подходе реджезации партонов получены в предложенной ранее авторами статьи модифицированной модели Кимбера — Мартина — Рыскина. При численных расчетах учитывается вклад только основного партонного процесса, $R + Q \to \gamma + q$, так как вклад других процессов не превышает 5–10 %. Результаты расчетов сравниваются с предсказаниями, полученными в коллинеарной партонной модели. Показано хорошее согласие расчетов в подходе реджезации партонов с экспериментальными данными, полученными коллаборацией ATLAS.

Ключевые слова: БАК; изолированные фотоны; жесткий процесс; партонная модель; подход реджезации партонов; квантовая хромодинамика.

Цитирование. Кузнецова А.А., Салеев В.А. Рождение изолированных фотонов с большими поперечными импульсами на БАК в реджевском пределе КХД // Вестник Самарского университета. Естественнонаучная серия. 2021. Т. 27, № 1. С. 104–110. DOI: http://doi.org/10.18287/2541-7525-2021-27-1-104-110.

Информация о конфликте интересов: авторы и рецензенты заявляют об отсутствии конфликта интересов.

© Кузнецова А.А., 2021
Алина Александровна Кузнецова — аспирант кафедры общей и теоретической физики, Самарский национальный исследовательский университет имени академика С.П. Королева, 443086, Российская Федерация, г. Самара, Московское шоссе, 34.

© Салеев В.А., 2021
Владимир Анатольевич Салеев — доктор физико-математических наук, профессор, заведущий кафедрой общей и теоретической физики, Самарский национальный исследовательский университет имени академика С.П. Королева, 443086, Российская Федерация, г. Самара, Московское шоссе, 34.

Введение

Теретическое и экспериментальное изучение процессов рождения прямых фотонов, т. е. фотонов, рождающихся непосредственно в жестких взаимодействиях кварков и глюонов из сталкивающихся протонов, представляет большой интерес для проверки пертурбативной квантовой хромодинамики (КХД) и исследования партонных (в первую очередь глюонных) функций распределения в протоне. В настоящее время накоплен богатый экспериментальный материал по спектрам фотонов по поперечному импульсу как в области относительно низких энергий (см. обзор [1]), так и при рекордно высоких энергиях Большого адронного коллайдера (БАК) [2–4]. В данной работе мы рассмотрим рождение прямых изолированных фотонов с большими поперечными импульсами на БАК при энергии 13 ТэВ [2]. В стандартной схеме расчетов сечений рождения прямых фотонов вычисления проводятся в коллинеарной партонной модели (КМП) в рамках теории возмущений по константе сильного взаимодействия α_S. В лидирующем приближении (ЛП) теории возмущений КХД рождение фотонов описывается процессами $q+\bar{q}\to\gamma+g$ и $q(\bar{q})+g\to\gamma+q(\bar{q})$ с К-фактором $K_{LO}\sim 2-3$. Учет следующих за лидирующими поправок (СЛП) улучшает согласие с данными, так что $K_{NLO}\sim 1.5$ [5]. Только в следующим за СЛП (ССЛП) приближении удается достичь количественного описания данных, $K_{NNLO}\sim 1.0$ [6]. Однако и в ССЛП-расчетах для лучшего согласия с экспериментальными данными в некоторых кинематических областях приходится наряду с хорошо определенным экспериментально конусным условием изоляции [2] вводить дополнительный феноменологический параметр — динамическое конусное условие [6], что делает описание крайне запутанным теоретически.

Ранее нами был предложен подход реджезации партонов (ПРП) [7; 8], который основан на теореме факторизации жестких процессов при высоких энергиях [9] и эффективной теории реджезованных глюонов и кварков Л.Н. Липатова [10]. Инклюзивное рождение прямых фотонов в ПРП исследовалось ранее в работах [11; 12]. В данной работе мы проводим расчеты спектров по поперечному импульсу изолированных прямых фотонов впервые. Условие изоляции формулируется следующим образом [2]: энергия конечных партонов внутри конуса радиуса $R_0=0.4$ вокруг направления движения фотона в координатах быстрота – азимутальный угол должна быть меньше $E_{ISO}=10$ Гэв. Условие попадания партона i внутрь конуса: $R_i=\sqrt{(\phi_i-\phi_\gamma)^2+(y_i-y_\gamma)^2}<R_0$. Сечение рождения изолированного фотона составляет только часть от инклюзивного сечения рождения, но использование условия изоляции при теоретических расчетах позволяет существенным образом уменьшить неопределенность, связанную с вкладом фрагментационных фотонов, которые испускаются конечными кварками по направлению своего движения. С экспериментальной точки зрения изучение изолированных фотонов также более строго определено в отличие от инклюзивной постановки эксперимента.

1. Подход реджезации партонов

ПРП основан на факторизации жестких процессов при высоких энергиях в условиях мультиреджевской кинематики, когда $\mu << \sqrt{S}$. Базовые положения подхода: k_T-факторизация при высоких энергиях, неинтегрированные ПФР, калибровочно-инвариантные партонные амплитуды в эффективной теории Л.Н. Липатова. Формула факторизации доказана в приближении главных логарифмических вкладов [9]. Неинтегрированные ПФР получены ранее [13] в модифицированной модели Кимбера — Мартина — Рыскина [14]. Внемассовые амплитуды партонных процессов строятся по правилам Фейнмана теории Л.Н. Липатова для реджезованных глюонов и кварков, что гарантирует их калибровочную инвариантность.

В ПРП сечение вычисляется по формуле

$$d\sigma \;=\; \sum_{i,\bar{j}}\int\limits_0^1\frac{dx_1}{x_1}\int\frac{d^2\mathbf{q}_{T1}}{\pi}\tilde{\Phi}_i(x_1,t_1,\mu^2)\int\limits_0^1\frac{dx_2}{x_2}\int\frac{d^2\mathbf{q}_{T2}}{\pi}\tilde{\Phi}_j(x_2,t_2,\mu^2)\cdot d\hat{\sigma}_{\rm PRA}, \tag{1}$$

где $t_{1,2}=-\mathbf{q}^2_{T1,2}$, сечение для реджезованных партонов $\hat{\sigma}_{\rm PRA}$ выражается через реджезованные амплитуды $\overline{|\mathcal{A}_{PRA}|^2}$. Неинтегрированные ПФР на древесном уровне $\tilde{\Phi}_i(x_{1,2},t_{1,2},\mu^2)$ в уравнении (1) вычисляются как свертка коллинеарных ПФР $f_i(x,\mu^2)$ и сплитинг-функций Докшицера — Грибова — Липатова — Алтарелли — Паризи (ДГЛАП) $P_{ij}(z)$ с фактором от t-канального обмена $1/t_{1,2}$,

$$\tilde{\Phi}_i(x,t,\mu)=\frac{\alpha_s(\mu)}{2\pi}\frac{1}{t}\sum_{j=q,\bar{q},g}\int\limits_x^1 dz\;\;P_{ij}(z)F_j\left(\frac{x}{z},\mu_F^2\right), \tag{2}$$

где $F_i(x,\mu_F^2)=xf_j(x,\mu_F^2)$. Здесь и далее мы полагаем, как обычно, $\mu_F=\mu_R=\mu$. Сечение (1) содержит коллинеарную расходимость при $t_{1,2}\to 0$ и инфракрасную расходимость при $z_{1,2}\to 1$.

Для регуляризации расходимостей модифицируем $\tilde{\Phi}_i(x,t,\mu)$ таким образом, чтобы новая неинтегрированная ПФР $\Phi_i(x,t,\mu)$ удовлетворяла точному условию нормировки:

$$\int\limits_0^{\mu^2} dt \Phi_i(x,t,\mu^2) = F_i(x,\mu^2), \tag{3}$$

что эквивалентно

$$\Phi_i(x,t,\mu^2) = \frac{d}{dt}\left[T_i(t,\mu^2,x)F_i(x,t)\right], \tag{4}$$

где $T_i(t,\mu^2,x)$ — форм-фактор Судакова, удоволетворяющий граничным условиям $T_i(t=0,\mu^2,x)=0$ and $T_i(t=\mu^2,\mu^2,x)=1$. Таким образом, модифицированная неинтегрированная ПФР принимает вид

$$\Phi_i(x,t,\mu) = \frac{\alpha_s(\mu)}{2\pi}\frac{T_i(t,\mu^2,x)}{t}\sum_{j=q,\bar{q},g}\int\limits_x^1 dz\ \ P_{ij}(z)F_j\left(\frac{x}{z},t\right)\theta\left(\Delta(t,\mu)-z\right). \tag{5}$$

Для регуляризации ИК-расходимости достаточно потребовать, чтобы $z_{1,2} < 1-\Delta_{KMR}(t_{1,2},\mu^2)$, где $\Delta_{KMR}(t,\mu^2) = \sqrt{t}/(\sqrt{\mu^2}+\sqrt{t})$. Это условие можно строго получить, если учесть, что в условии мультиреджевской кинематики доминирует вклад процессов упорядоченных по быстроте $y_q > y_{\mathcal{Y}} > y_{\bar{q}}$ [13].

Решение уравнения для форм-фактора Судакова дает

$$T_i(t,\mu^2,x) = \exp\left[-\int\limits_t^{\mu^2}\frac{dt'}{t'}\frac{\alpha_s(t')}{2\pi}\left(\tau_i(t',\mu^2)+\Delta\tau_i(t',\mu^2,x)\right)\right], \tag{6}$$

где

$$\begin{aligned}
\tau_i(t,\mu^2) &= \sum_j\int\limits_0^1 dz\ \ zP_{ji}(z)\theta(\Delta(t,\mu^2)-z),\\
\Delta\tau_i(t,\mu^2,x) &= \sum_j\int\limits_0^1 dz\ \ \theta(z-\Delta(t,\mu^2))\left[zP_{ji}(z)-\frac{F_j\left(\frac{x}{z},t\right)}{F_i(x,t)}P_{ij}(z)\theta(z-x)\right].
\end{aligned}$$

Несколько лет назад был предложен численный метод получения калибровочно-инвариантных амплитуд рассеяния с участием реджезованных партонов, который использует технику спиральных амплитуд и рекуррентные соотношения, подобные BCFW [15; 16]. На основе предложенного метода был разработан Монте — Карло генератор партонного уровня KaTie [17]. Как было показано ранее [7], этот метод для численной генерации амплитуд с внемассовыми партонами в начальном состоянии (t-канальные глюоны) эквивалентен эффективной теории Л.Н. Липатова на уровне древесных диаграмм. Для партонных процессов $2\to 3$ или $2\to 4$ численный метод генерации амплитуд более эффективен, чем полуаналитические расчеты по фейнмановским правилам эффективной теории при описании процессов рождения фотонов и струй. Однако для описания наблюдаемых фотонов, связанных, например, с тяжелыми кваркониями, метод фейнмановских диаграмм эффективной теории Л.Н. Липатова оказывается единственно возможным, как и для расчетов в СЛП приближении ПРП NLO [18]. Представленные ниже результаты вычислений получены с использованием генератора KaTie, но мы используем оригинальные неинтегрированные ПФР [13].

2. Результаты расчетов

В ЛП ПРП рождение прямого изолированного фотона описывается такими же процессами, как и в КПМ, но с заменой начальных партонов на реджезованные:

$$Q(\bar{Q}) + R \to \gamma + q(\bar{q}), \tag{7}$$
$$Q + \bar{Q} \to \gamma + g. \tag{8}$$

При высоких энергиях вклад процесса (7) является доминирующим (~ 90 %), т. к. глюонные ПФР в области малых x значительно превышают по величине карковые ПФР. Расчет заведомо малого вклада процесса (8) будет выполнен на следующем этапе исследования.

Экспериментальные данные коллаборации ATLAS [4; 2] для дифференциального сечения рассеяния по поперечному импульсу изолированного фотона получены для четырех интервалов по быстроте фотона: $|y|<0.6,\ 0.6<|y|<1.37,\ 1.56<|y|<1.81,\ 1.81<|y|<2.37$. Результаты расчетов в ЛП ПРП при

выборе жесткого масштаба $\mu = p_T$ сравниваются с экспериментальными данными на рис. 2.1–2.4 для энергии $\sqrt{S} = 13$ ТэВ.

Во всех интервалах по быстроте предсказания ЛП ПРП, а также полученные в СЛП КМП, при $p_T \geqslant 800$ ГэВ незначительно превышают экспериментальные данные, что может указывать на неточность параметризаций глюонных и кварковых ПФР при больших $x > 0.5$. Этой же причиной можно объяснить превышение над экспериментальными данными при всех p_T в области больших быстрот, см. Рис. 2.4. В областях быстрот $|y| < 0.6$ и $1.56 < |y| < 1.81$ ПРП значительно лучше описывает экспериментальные данные, чем расчеты в СЛП КМП.

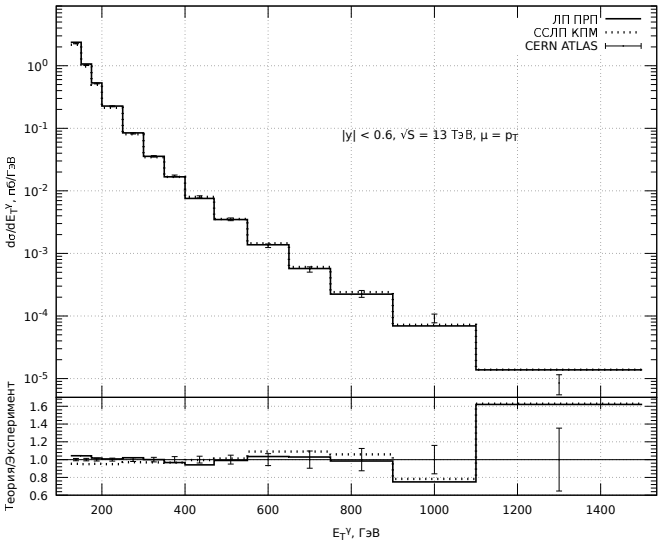

Рис. 2.1. Дифференциальное сечение рождения изолированных фотонов при энергии $\sqrt{s} = 13$ ТэВ и $|y| < 0.6$ как функция поперечного импульса. Теоретические расчеты в ЛП ПРП [13], в СЛП КПМ [19; 20]. Экспериментальные данные коллаборации ATLAS [2]

Fig. 2.1. Differential cross section for the production of isolated photons at energy $\sqrt{s} = 13$ TeV and $|y| < 0.6$ as a function of transverse momentum. Theoretical calculations in LP PRP [13], in SLP KPM [19; 20]. Experimental data of the ATLAS collaboration [2]

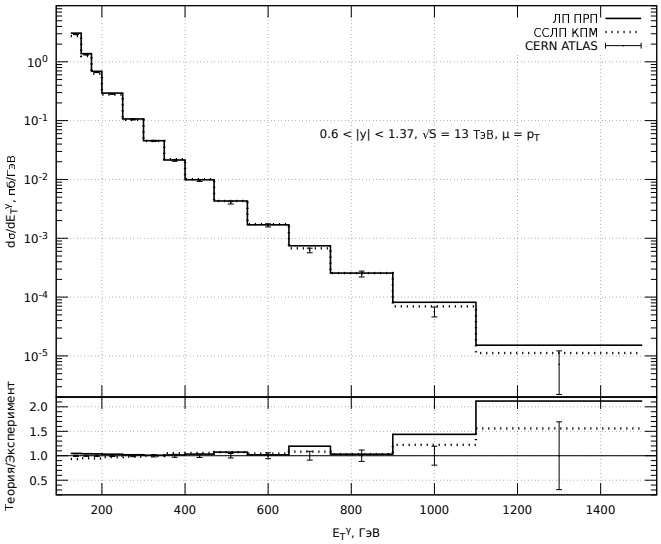

Рис. 2.2. Дифференциальное сечение рождения изолированных фотонов при энергии $\sqrt{s} = 13$ ТэВ и $0.6 < |y| < 1.37$ как функция поперечного импульса

Fig. 2.2. Differential cross section for the production of isolated photons at energy $\sqrt{s} = 13$ TeV and $0.6 < |y| < 1.37$ as a function of transverse momentum

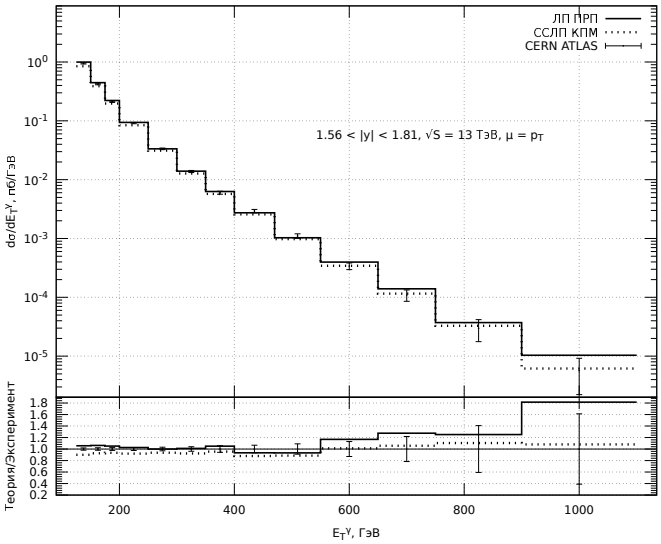

Рис. 2.3. Дифференциальное сечение рождения изолированных фотонов при энергии $\sqrt{s} = 13$ ТэВ и $1.56 < |y| < 1.81$ как функция поперечного импульса
Fig. 2.3. Differential cross section for the production of isolated photons at energy $\sqrt{s} = 13$ TeV and $1.56 < |y| < 1.81$ as a function of transverse momentum

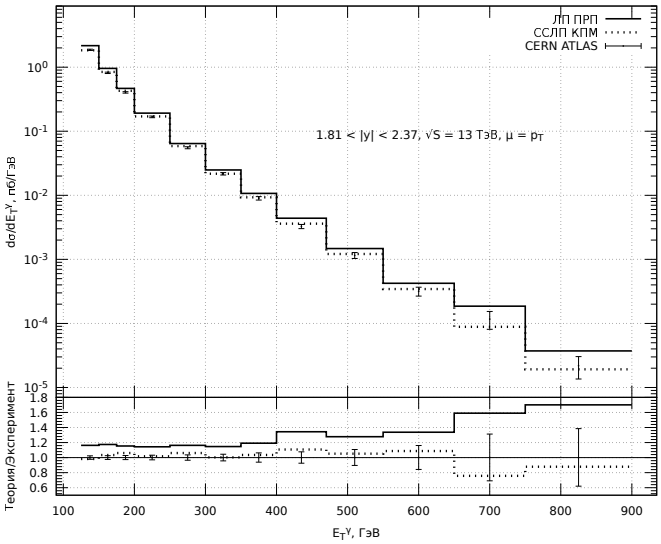

Рис. 2.4. Дифференциальное сечение рождения изолированных фотонов при энергии $\sqrt{s} = 13$ ТэВ и $1.81 < |y| < 2.37$ как функция поперечного импульса
Fig. 2.4. Differential cross section for the production of isolated photons at energy $\sqrt{s} = 13$ TeV and $1.81 < |y| < 2.37$ as a function of transverse momentum

Выводы

Проведен расчет дифференциальных сечений рождения по поперечному импульсу изолированных фотонов с большими поперечными импульсами на БАК в реджевском пределе КХД в рамках ЛП ПРП. Показано, что согласие с экспериментальными данными коллаборации ATLAS [2] в некоторых областях быстрот фотонов даже превосходит по точности результаты расчетов в СЛП КПМ. Показано, что предложенные ранее модифицированные глюонные и кварковые неинтегрированные ПФР [13] могут быть эффективно использованы в расчетах в ПРП.

Благодарности

Авторы благодарны Максиму Нефедову за консультации по вопросам использования новых неинтегрированных ПФР в модели КМР и Александре Шипиловой за помощь в установке программы KaTie. Работа выполнена при поддержке Министерства науки и высшего образования Российской Федерации, проект FSSS-2020-0014.

Литература / References

[1] Vogelsang W., Whalley M.R. A compilation of data on single and double prompt photon production in hadron-hadron interactions. *J. Phys. G: Nucl. Part. Phys.*, 1997, vol. 23, A1–A69. Available at: https://iopscience.iop.org/article/10.1088/0954-3899/23/7A/001.

[2] Aad G. [et al.] Measurement of the inclusive isolated-photon cross section in pp collisions at $\sqrt{s} = 13$ TeV using 36 fb^{-1} of ATLAS data. *Journal of High Energy Physics*, 2019, Issue 10. DOI: https://doi.org/10.1007/jhep10(2019)203.

[3] CMS collaboration, Measurement of differential cross sections for inclusive isolated-photon and photon+jets production in proton-proton collisions at v s = 13 TeV. *Eur. Phys. J. C Part Fields*, 2019, vol. 79, no. 1, p. 20. DOI: 10.1140/epjc/s10052-018-6482-9.

[4] G. Aad [et al.] Measurement of the inclusive isolated prompt photon cross section in pp collisions at $\sqrt{s} = 8$ TeV with the ATLAS detector. *Journal of High Energy Physics*, 2016, Issue 08. DOI: http://dx.doi.org/10.1007/JHEP08(2016)005.

[5] Fontannaz M., Guillet J.P., Heinrich G. Isolated prompt photon photoproduction at NLO. *Eur. Phys. J. C Part Fields*, 2001, vol. 21, no. 2, pp. 303–312. DOI: http://dx.doi.org/10.1007/s100520100732.

[6] X. Chen [et al.] Isolated photon and photon+jet production at NNLO QCD accuracy. *Journal of High Energy Physics*, 2020, Issue 04, p. 166. DOI: http://dx.doi.org/10.1007/jhep04(2020)166.

[7] Nefedov M.A., Saleev V.A., Shipilova A.V. Dijet azimuthal decorrelations at the LHC in the parton Reggeization approach. *Physical Review D: Particles and fields*, 2013, Vol. 87, no. 9, p. 094030. DOI: http://dx.doi.org/10.1103/PhysRevD.87.094030.

[8] Karpishkov A.V., Nefedov M.A., Saleev V.A. $B\bar{B}$ angular correlations at the LHC in parton Reggeization approach merged with higher-order matrix elements. *Physical Review D: Particles and fields*, 2017, Vol. 96, no. 9, p. 096019. http://dx.doi.org/10.1103/PhysRevD.96.096019.

[9] Collins J.C., Ellis R.K. Heavy quark production in very high-energy hadron collisions. *Nuclear Physics B*, 1991, Vol. 360, issue 1, pp. 3–30. DOI: https://doi.org/10.1016/0550-3213%2891%2990288-9

[10] Lipatov L.N. Gauge invariant effective action for high-energy processes in QCD. *Nuclear Physics B*, 1995, 452, issues 1–2, pp. 369–397. DOI: https://doi.org/10.1016/0550-3213(95)00390-E.

[11] Saleev V.A. Deep inelastic scattering and prompt photon production within the framework of quark Reggeization hypothesis. *Physical Review D: Particles and fields*, 2008, 78, p. 034033. DOI: http://dx.doi.org/10.1103/PhysRevD.78.034033.

[12] B.A. Kniehl [et al.] Single jet and prompt-photon inclusive production with multi-Regge kinematics: From Tevatron to LHC. *Physical Review D: Particles and fields*, 2011, Vol. 84, p. 074017. DOI: http://dx.doi.org/10.1103/PhysRevD.84.074017.

[13] Nefedov M.A., Saleev V.A. High-Energy Factorization for Drell-Yan process in pp and $p\bar{p}$ collisions with new Unintegrated PDFs. *Physical Review D: Particles and fields*, 2020, Vol. 102, p. 114018. DOI: https://doi.org/10.1103/physrevd.102.114018.

[14] Kimber M.A., Martin A.D., Ryskin M.G. Unintegrated parton distributions. *Physical Review D: Particles and fields*, 2001, Vol. 63, p. 114027. DOI: https://doi.org/10.1103/PhysRevD.63.114027.

[15] Hameren van A., Kotko P., Kutak K. Helicity amplitudes for high-energy scattering. *Journal of High Energy Physics*, 2013, Issue 01, p. 078. DOI: http://Doi.org/10.1007/JHEP01(2013)078.

[16] Hameren van A., Kutak K., Salwa T. Scattering amplitudes with off-shell quarks. *Physics Letters B.*, 2013, Vol. 727, no. 1–3, pp. 226–233. DOI: http://dx.doi.org/10.1016/j.physletb.2013.10.039.

[17] Hameren van A. KaTie: For parton-level event generation with k_T-dependent initial states. *Computer Physics Communications*, 2018, 224, pp. 371–380. DOI: http://dx.doi.org/10.1016/j.cpc.2017.11.005.

[18] Nefedov M., Saleev V. On the one-loop calculations with Reggeized quarks. *Modern Physics Letters A.*, 2017, 32, no. 40, p. 1750207. DOI: http://dx.doi.org/10.1142/S0217732317502078.

[19] Sjostrand T., Mrenna S., Skands P.Z. A Brief Introduction to PYTHIA 8.1. *Computer Physics Communications*, 2008, 178, no. 11, pp. 852–867. DOI: http://dx.doi.org/10.1016/j.cpc.2008.01.036.

[20] T. Gleisberg [et al.] Event generation with SHERPA 1.1. *Journal of High Energy Physics*, 2009, Issue 0902, p. 007. DOI: https://doi.org/10.1088/1126-6708%2F2009%2F02%2F007.

Scientific article

DOI: 10.18287/2541-7525-2021-27-1-104-110

Submited: 07.01.2021
Revised: 04.02.2021
Accepted: 28.02.2021

A.A. Kuznetsova
Samara National Research University, Samara, Russian Federation
E-mail: malina-jun@yandex.ru. ORCID: https://orcid.org/0000-0002-3670-2499
V.A. Saleev
Samara National Research University, Samara, Russian Federation
E-mail: saleev@samsu.ru. ORCID: https://orcid.org/0000-0003-0505-5564

PRODUCTION OF ISOLATED PHOTONS WITH LARGE TRANSVERSE MOMENTA AT LHC IN THE REGGE LIMIT OF QCD

ABSTRACT

The article discusses the production of prompt isolated photons with large transverse momenta at the LHC at energies $\sqrt{s} = 8$ and 13 TeV in the parton Reggeization approach, which is based on the factorization theorem for hard processes at high energies and the effective theory of Reggeized gluons and quarks by L.N. Lipatov. Unintegrated parton distributions in the parton Reggeization approach were obtained in the modified Kimber–Martin–Ryskin model proposed earlier by the authors of the article. In numerical calculations, only the contribution of the main parton process, $R + Q(\bar{Q}) \to \gamma + q(\bar{q})$, is taken into account, since the contribution of other processes does not exceed 5–10 %. The calculation results are compared with the predictions obtained in the collinear parton model. Good agreement of calculations in the parton Reggeization approach with experimental data obtained by the ATLAS collaboration is shown.

Key words: LHC; isolated photons; hard process; parton model; parton Reggeization approach; quantum chromodynamics.

Citation. Kuznetsova A.A., Saleev V.A. Production of isolated photons with large transverse momenta at LHC in the Regge limit of QCD. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2021, vol. 27, no. 1, pp. 104–110. DOI: http://doi.org/10.18287/2541-7525-2021-27-1-104-110. (In Russ.)

Information about the conflict of interests: authors and reviewers declare no conflict of interests.

© Kuznetsova A.A., 2021
Alina Alexandrovna Kuznetsova — postgraduate student of the Department of General and Theoretical Physics, Samara National Research University, 34, Moskovskoye shosse, Samara, 443086, Russian Federation.
© Saleev V.A., 2021
Vladimir Anatolievich Saleev — Doctor of Physical and Mathematical Sciences, professor, head of the Department of General and Theoretical Physics, Samara National Research University, 34, Moskovskoye shosse, Samara, 443086, Russian Federation.

ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ СТАТЕЙ

Журнал "Вестник Самарского университета. Естественнонаучная серия" издается с 1995 г. и является регулярным научным изданием, выпускаемым Самарским университетом с целью развития научно-исследовательской деятельности, поддержки ведущих научных школ и подготовки кадров высшей квалификации. Журнал выходит как в печатном, так и в электронном виде. Электронная версия журнала размещается на сайте Самарского университета по адресу *http://vestnik.samsu.ruhttp://journals.ssau.ru/index.php/vestnik-est*. Все статьи проходят проверку в программе "Антиплагиат".

В журнале "Вестник Самарского университета. Естественнонаучная серия" печатаются оригинальные научные результаты из различных областей естествознания по профилю базы данных zbMath, ранее не публиковавшиеся и не представленные к публикации в других изданиях. **Ежегодно выходят в свет четыре регулярных выпуска журнала.**

Представляемая в журнал работа должна быть законченным научным исследованием и содержать новые научные результаты. Статьи должны подписываться всеми авторами, что означает их согласие на передачу всех прав на распространение работ с помощью печатных и электронных носителей информации Самарскому университету. Статьи могут быть написаны на русском или английском языках, при этом авторы обязаны предъявлять повышенные требования к стилю изложения и языку. Статьи должны сопровождаться направлением организации, в которой выполнена работа. Статьи обзорного характера, рецензии на научные монографии пишутся, как правило, по просьбе редколлегии журнала. Все представленные работы редакция журнала направляет на рецензирование. Решение об опубликовании принимается редколлегий журнала на основании рецензии. Авторам рекомендуется ознакомиться с правилами подготовки статей перед представлением их в редакцию. Работы, оформленные не по правилам, редколлегией рассматриваться не будут. **Редакция просит авторов при оформлении работы придерживаться следующих правил и рекомендаций:**

1. Статьи представляются в двух форматах: твердая копия, распечатанная с одной стороны листа формата А4, и электронная (e-mail: nsvestnik@ssau.ru). Электронный вариант должен точно соответствовать печатному.

2. Статья должна содержать: название работы (без формул), список авторов, представленный в алфавитном порядке, с указанием места работы и его адреса с индексом, адресов электронной почты каждого из них, звания, должности, ORCID на русском и английском языках; аннотацию не менее 100 слов на русском и английском языках, которая дается перед основным текстом; основной текст, который рекомендуется разделять на подразделы с целью облегчения чтения работы; заключение с краткой характеристикой основных полученных результатов.

3. Статья должна быть снабжена индексом универсальной классификации (УДК), необходимо представить ключевые слова на русском и английском языках.

4. Объем статьи не должен превышать 15–25 страниц, иллюстрированного не более чем 5 рисунками и 5 таблицами. Базовый размер шрифта — 10 пунктов. Опубликование работ, не соответствующих этим ограничениям, возможно только после специального решения редколлегии журнала.

5. Подписи к рисункам должны размещаться снизу от рисунка и должны содержать их краткое описание и, возможно, объяснение использованных символов и условных обозначений.

6. Указатель таблицы должен быть размещен справа сверху от таблицы. Заголовок таблицы (как и сама таблица) должен быть отцентрирован по ширине основного текста.

7. Нумерация рисунков и таблиц должна быть пораздельной по тексту статьи. Не допускается размещать в тексте рисунки и таблицы до появления на них ссылки в тексте.

8. Текст статьи должен быть подготовлен средствами издательской системы LaTeX2$_\varepsilon$ с использованием стиля `samgu.cls`. Стиль `samgu.cls` и пример оформления статьи можно найти на сайте Самарского государственного университета (адрес указан выше). Использование других реализаций TeX'а крайне нежелательно. Подготовка электронной версии статьи с помощью других средств должна быть заранее согласована с редакцией. Иллюстративный материал (рисунки, таблицы, диаграммы) готовится стандартными средствами LaTeX'а. Рисунки могут быть также подготовлены в любом графическом редакторе и предоставлены в формате EPS. Электронные представления фотографий допускаются только в форматах EPS или TIFF с разрешением не менее 600 dpi. В случае использования нестандартных стилевых файлов автор обязан предоставить редакции необходимые стилевые файлы. Изменения стандартных стилевых файлов недопустимы.

9. При подготовке электронного варианта статьи следует принимать во внимание следующие рекомендации:

а) при наборе статьи необходимо различать следующие знаки препинания и контрольные последовательности, им соответствующие: одинарный дефис ("-"), двойной дефис ("–")[1], тройной дефис ("—")[2]. Одинарный дефис используют в составных словах; двойной дефис рекомендуется для указания диапазона чисел и "двойных"фамилий; тройной дефис означает тире;

б) допустимо использование только обратных кавычек (") с помощью контрольной последовательности `\textquotedblright`;

в) недопустимо нахождения рядом двух и более закрывающих или открывающих скобок одного вида. Рекомендуется внимательно относиться к балансу скобок;

г) допускается использование следующих команд переключения шрифтов: `\rm`, `\it`, `\bf`, `\sl` и стандартных шрифтов семейства AMS с использованием следующих команд переключения шрифтов `\mathbf`, `\mathcal`, `\mathfrak`. Использование других шрифтов должно быть согласовано с редакцией журнала;

д) на графиках должна быть нанесена сетка (желательно квадратная) с обозначением делений. Рекомендуемый размер рисунков — 11-15 см по горизонтали и 5-15 см по вертикали. Необходимо тщательно следить за точным соответствием обозначений в тексте и на рисунках и за подобием шрифтов. Надписи, загромождающие рисунки, должны

[1]Соответствующая контрольная последовательность есть `\cdash--~`

[2]Соответствующая контрольная последовательность есть `\cdash---`

быть заменены цифрами или буквенными обозначениями и внесены в подрисуночные подписи. Сами подрисуночные подписи должны быть, по возможности, краткими. Редакция оставляет за собой право требовать от автора более качественного выполнения графического материала;

е) для математических обозначений рекомендуется употреблять, по возможности, стандартные и наиболее простые символы. Не следует применять индексы из букв русского алфавита. Векторы и тензоры выполняются жирным шрифтом. Вместо одинаковых повторяющихся блоков в формулах желательно использовать их сокращенные обозначения;

ж) при нумерации формул редакция просит пользоваться десятичной системой. Рекомендуется двойная нумерация: первая цифра — номер раздела статьи, вторая цифра после точки — номер формулы внутри раздела. Номер должен стоять справа от формулы. Не следует нумеровать формулы, на которые нет ссылок в тексте;

з) теоремы, леммы, примеры, утверждения и т.п. выполняются обычным шрифтом; их заголовки даются жирным шрифтом;

и) список литературы составляется по порядку цитирования, располагается в конце статьи на русском и английском языках (не менее 10 пунктов). Для книг сообщается следующая информация: фамилии и инициалы авторов, полное название книги, издательство, год издания и количество страниц; для статей в сборниках и журналах — фамилии и инициалы авторов, полное название статьи, название журнала (сборника) полностью или, если есть стандартное сокращение, сокращенно, полная информация об издании (серия, том, номер, выпуск, год), номера начальной и конечной страниц статьи;

к) ссылки на иностранные источники (включая переведенные на русский язык статьи и книги) даются обязательно на языке оригинала и сопровождаются в случае перевода на русский язык с указанием названия и выходных данных перевода.

Цитирование осуществляется командой `\cite` с соответствующей меткой. Ссылки на неопубликованные работы недопустимы.

Невыполнение авторами перечисленных выше правил может повлечь за собой задержку с опубликованием работы.

В журнале дается указание на дату поступления работы в редакцию и даты ее принятия. Просьба редакции о переработке статьи не означает, что статья принята к печати; после переработки статья вновь рассматривается редколлегией журнала.

Редакция журнала