

Министерство образования и науки Российской Федерации
Ярославский государственный университет им. П. Г. Демидова

МОДЕЛИРОВАНИЕ И АНАЛИЗ ИНФОРМАЦИОННЫХ СИСТЕМ

Том 25 № 3 (75) 2018

Основан в 1999 году
Выходит 6 раз в год

Главный редактор

В.А. Соколов,

доктор физико-математических наук, профессор, Россия

Редакционная коллегия

С.М. Абрамов, д-р физ.-мат. наук, чл.-корр. РАН, Россия; **Л. Авено**, проф., Франция;
В.С. Афраймович, проф.-исследователь, Мексика; **О.Л. Бандман**, д-р техн. наук, Россия;
В.Н. Белых, д-р физ.-мат. наук, проф., Россия; **В.А. Бондаренко**, д-р физ.-мат. наук, проф., Россия; **С.Д. Глызин**, д-р физ.-мат. наук, проф., Россия (зам. гл. ред.); **А. Дехтярь**, проф., США; **М.Г. Дмитриев**, д-р физ.-мат. наук, проф., Россия; **В.Л. Дольников**, д-р физ.-мат. наук, проф., Россия; **В.Г. Дурнев**, д-р физ.-мат. наук, проф., Россия; **В.А. Захаров**, д-р физ.-мат. наук, проф., Россия; **Л.С. Казарин**, д-р физ.-мат. наук, проф., Россия; **Ю.Г. Карпов**, д-р техн. наук, проф., Россия; **С.А. Кашенко**, д-р физ.-мат. наук, проф., Россия; **А.Ю. Колесов**, д-р физ.-мат. наук, проф., Россия; **Н.А. Кудряшов**, д-р физ.-мат. наук, проф., Заслуженный деятель науки РФ, Россия; **О. Кушнаренко**, проф., Франция; **И.А. Ломазова**, д-р физ.-мат. наук, проф., Россия; **Г.Г. Малинецкий**, д-р физ.-мат. наук, проф., Россия; **В.Э. Малышкин**, д-р техн. наук, проф., Россия; **А.В. Михайлов**, д-р физ.-мат. наук, проф., Великобритания; **В.А. Непомнящий**, канд. физ.-мат. наук, Россия; **Н.Х. Розов**, д-р физ.-мат. наук, проф., чл.-корр. РАО, Россия; **Н. Сидорова**, д-р наук, Нидерланды; **Р.Л. Смелянский**, д-р физ.-мат. наук, проф., член-корр. РАН, академик РАЕН, Россия; **Е.А. Тимофеев**, д-р физ.-мат. наук, проф., Россия (зам. гл. ред.); **М.Б. Трахтенброт**, д-р комп. наук, Израиль; **Д.В. Тураев**, проф., Великобритания; **Ф. Шнеблен**, проф., Франция

Ответственный секретарь **Е. В. Кузьмин**, д-р физ.-мат. наук, проф., Россия

Адрес редакции: ЯрГУ, ул. Советская, 14, г. Ярославль, 150003, Россия
Website: <http://mais-journal.ru>, e-mail: mais@uniyar.ac.ru; телефон (4852) 79-77-73

Научные статьи в журнал принимаются по электронной почте. Статьи должны содержать УДК, аннотации на русском и английском языках и сопровождаться набором текста в редакторе LaTeX. Плата с аспирантов за публикацию рукописей не взимается.

СОДЕРЖАНИЕ

Моделирование и анализ информационных систем. Т. 25, №3. 2018

Программно-конфигурируемые сети

Новый подход к обнаружению и устранению аномалий в политике безопасности внешнего модуля межсетевого экрана контроллера ПКС Floodlight

Моржов С. В., Никитинский М. А.

251

Вероятностные модели

Об оценке средней временной выгоды в вероятностных эколого-экономических моделях

Родина Л. И., Тютеев И. И.

257

Динамические системы

Динамика распределения популяции по ареалам

Кириллов А. Н., Данилова И. В.

268

Криптосистемы

Об алгоритме расщепления носителя для индуцированных кодов

Косолапов Ю. В., Шигаев А. Н.

276

Вычислительная геометрия

Об оптимальной интерполяции линейными функциями на n -мерном кубе

Невский М. В., Узалов А. Ю.

291

О гипотезах Ходжа, Тэйта и Мамфорда–Тэйта для расслоенных произведений семейств регулярных поверхностей с геометрическим родом 1

Орешкина (Никольская) О. В.

312

Теория функций

О дифференцируемости по Тейлору в пространствах $L_p, 0 < p \leq \infty$

Морозов А. Н.

323

Изопериметрические и функциональные неравенства

Климов В. С.

331

Свидетельство о регистрации СМИ ПИ № ФС 77 – 66186 от 20.06.2016 выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций. Учредитель – Федеральное государственное бюджетное образовательное учреждение высшего образования "Ярославский государственный университет им. П. Г. Демидова". Подписной индекс – 31907 в Объединенном каталоге "Пресса России". Редактор, корректор А. А. Аладьева. Редактор перевода Э. И. Соколова. Подписано в печать 18.06.2018. Дата выхода в свет 30.06.2018. Формат 60x84¹/₈. Усл. печ. л. 11,1. Уч.-изд. л. 10,0. Объем 96 с. Тираж 46 экз. Свободная цена. Заказ 046/018. Адрес типографии: ул. Советская, 14, оф. 109, г. Ярославль, 150003 Россия. Адрес издателя: Ярославский государственный университет им. П. Г. Демидова, ул. Советская, 14, г. Ярославль, 150003 Россия.

ISSN 1818–1015 (Print)
ISSN 2313–5417 (Online)

P.G. Demidov Yaroslavl State University

MODELING AND ANALYSIS OF INFORMATION SYSTEMS

Volume 25 No 3 (75) 2018

Founded in 1999
6 issues per year

Editor-in-Chief

V. A. Sokolov,

Doctor of Sciences in Mathematics, Professor, Russia

Editorial Board

S.M. Abramov, Prof., Dr. Sci., Corr. Member of RAS, Russia; **V. Afraimovich**, Prof.-researcher, Mexico; **L. Aveneau**, Prof., France; **O.L. Bandman**, Prof., Dr. Sci., Russia; **V.N. Belykh**, Prof., Dr. Sci., Russia; **V.A. Bondarenko**, Prof., Dr. Sci., Russia; **S.D. Glyzin**, Prof., Dr. Sci., Russia (*Deputy Editor-in-Chief*); **A. Dekhtyar**, Prof., USA; **M.G. Dmitriev**, Prof., Dr. Sci., Russia; **V.L. Dol'nikov**, Prof., Dr. Sci., Russia; **V.G. Durnev**, Prof., Dr. Sci., Russia; **L.S. Kazarin**, Prof., Dr. Sci., Russia; **Yu.G. Karpov**, Prof., Dr. Sci., Russia; **S.A. Kashchenko**, Prof., Dr. Sci., Russia; **A.Yu. Kolesov**, Prof., Dr. Sci., Russia; **O. Kouchnarenko**, Prof., France; **N.A. Kudryashov**, Dr. Sci., Prof., Russia; **I.A. Lomazova**, Prof., Dr. Sci., Russia; **G.G. Malinetsky**, Prof., Dr. Sci., Russia; **V.E. Malyshkin**, Prof., Dr. Sci., Russia; **A.V. Mikhailov**, Prof., Dr. Sci., Great Britain; **V.A. Nepomniaschy**, PhD, Russia; **N.H. Rozov**, Prof., Dr. Sci., Corr. Member of RAE, Russia; **Ph. Schnoebelen**, Senior Researcher, France; **N. Sidorova**, Dr., Assistant Prof., Netherlands; **R.L. Smeliansky**, Prof., Dr. Sci., Corr. Member of RAS, Russia; **E.A. Timofeev**, Prof., Dr. Sci., Russia (*Deputy Editor-in-Chief*); **M. Trakhtenbrot**, Dr., Israel; **D. Turaev**, Prof., Great Britain; **V.A. Zakharov**, Prof., Dr. Sci., Russia

Responsible Secretary **E. V. Kuzmin**, Prof., Dr. Sci., Russia

Editorial Office Address: P.G. Demidov Yaroslavl State University,
14 Sovetskaya str., Yaroslavl 150003, Russia
Website: <http://mais-journal.ru>, e-mail: mais@uniyar.ac.ru

© P.G. Demidov Yaroslavl State University, 2018

Contents

Modeling and Analysis of Information Systems. Vol. 25, No 3. 2018

Software Defined Networks

- A New Approach for Detecting and Resolving Anomalies in Security Policy
of the External Firewall Module of the Floodlight SDN Controller
Morzhov S. V., Nikitinskiy M. A. 251

Probabilistic Models

- On Estimation of an Average Time Profit in Probabilistic Environmental and Economic Models
Rodina L. I., Tyuteev I. I. 257

Dynamical Systems

- Dynamics of Population Patch Distribution
Kirillov A. N., Danilova I. V. 268

Cryptosystems

- The Support Splitting Algorithm for Induced Codes
Kosolapov Yu. V., Shigaev A. N. 276

Computational Geometry

- On Optimal Interpolation by Linear Functions on an n -Dimensional Cube
Nevskii M. V., Ukhlov A. Yu. 291

- On the Hodge, Tate and Mumford-Tate Conjectures for Fibre Products
of Families of Regular Surfaces with Geometric Genus 1
Oreshkina (Nikol'skaya) O. V. 312

Function Theory

- On the Taylor Differentiability in Spaces $L_p, 0 < p \leq \infty$
Morozov A. N. 323

- Isoperimetric and Functional Inequalities
Klimov V. S. 331

Программно-конфигурируемые сети

©Morzhov S. V., Nikitinskiy M. A., 2017

DOI: 10.18255/1818-1015-2018-3-251-256

UDC 004.415.25

A New Approach for Detecting and Resolving Anomalies in Security Policy of the External Firewall Module of the Floodlight SDN Controller

Morzhov S. V., Nikitinskiy M. A.¹

Received December 26, 2017

Abstract. In this paper, the authors analyze the developed PreFirewall network application for the Floodlight *software defined network* (SDN) controller. This application filters rules, which are added into the firewall module of the Floodlight SDN controller in order to prevent the occurrence of anomalies among them. The rule filtering method is based on determining whether the addition of a new rule will not cause any anomalies with already added ones. If an anomaly was detected while adding the new rule, PreFirewall application should be able to resolve it and must report the detection of the anomaly.

The developed network application PreFirewall passed a number of tests. As a result of the stress testing, it was found that the time of adding a new rule, when using PreFirewall, substantially increases with increase in the number of previously processed rules. Analysis of the network application PreFirewall showed that while adding a rule (the most frequent operation), in the worst case it is necessary to compare it with all existing rules, which are stored as a two-dimensional array. Thus, the operation of adding a new rule is the most time-consuming and has the greatest impact on the performance of the network application, which leads to an increase in response time.

A possible way to of solving this problem is to select a data structure used to store the rules, in which the operation of adding a new rule would be simple. After analyzing the structure of the policy rules for the Floodlight SDN controller, the authors noted that a tree is the most adequate data structure for its storage. It provides optimization of memory used for storing the rules and, more important, it allows to achieve the constant complexity of the operation of adding a new rule and, consequently, solving the performance problem of the network application PreFirewall.

The article is published in the authors' wording.

Keywords: firewall, Floodlight, hash table, network controller, policy tree, PreFirewall, rules anomalies resolving, SDN, software-defined network

For citation: Morzhov S. V., Nikitinskiy M. A., "A New Approach for Detecting and Resolving Anomalies in Security Policy of the External Firewall Module of the Floodlight SDN Controller", *Modeling and Analysis of Information Systems*, 25:3 (2018), 251–256.

On the authors:

Sergey V. Morzhov, orcid.org/0000-0001-6652-3574, graduate student,
P.G. Demidov Yaroslavl State University,
14 Sovetskaya str., Yaroslavl 150003, Russia, e-mail: smorzhov@gmail.com

Mikhail A. Nikitinskiy, orcid.org/0000-0001-8830-8613, system analyst, programmer,
A-Real Group, Energiya-Info Inc., 144 Soyuznaya str., Yaroslavl, 150008, Russia, e-mail: man@a-real.ru

Acknowledgments:

¹The work was supported by RFBR, the research project № 16-07-01103a.

Introduction

The Prefirewall network application for the SDN FloodLight controller [1], proposed by the authors in the article [2], showed good results in filtering the added rules in policies rule sets. The developed algorithm prevents the occurrence of any anomalies among them. However, the load testing of the network application revealed a serious drawback in it – an increasing time the application spent to add a new rule when the number of processed rules is big enough.

To test the network application, 15 000 rules were created by the random rule generator. Such an amount of rules was proposed by one of the Russian manufacturer of UTM (*Unified threat management*) solutions, based on an analysis of the rule sets used in customer organizations with an average of 500 users. Testing was performed on a computer running Ubuntu 14.04 with Intel core i7 processor with a clock rate of 3 GHz.

Firstly, the time taken to load all generated rules directly into the external module of the Floodlight SDN controller was measured. After that, the same rules have been added to the Floodlight through PreFirewall network application, which resolves all the anomalies between them. Fig. 1 illustrates how the time taken to add each rule is growing with the growth of the number of processed and stored rules. On the *x-axis*, the scale values are from 0 to 15 000 and shows the number of installed rules. On the *y-axis*, the scale values are from 0 to 2.5 and show the rule installation time in seconds.

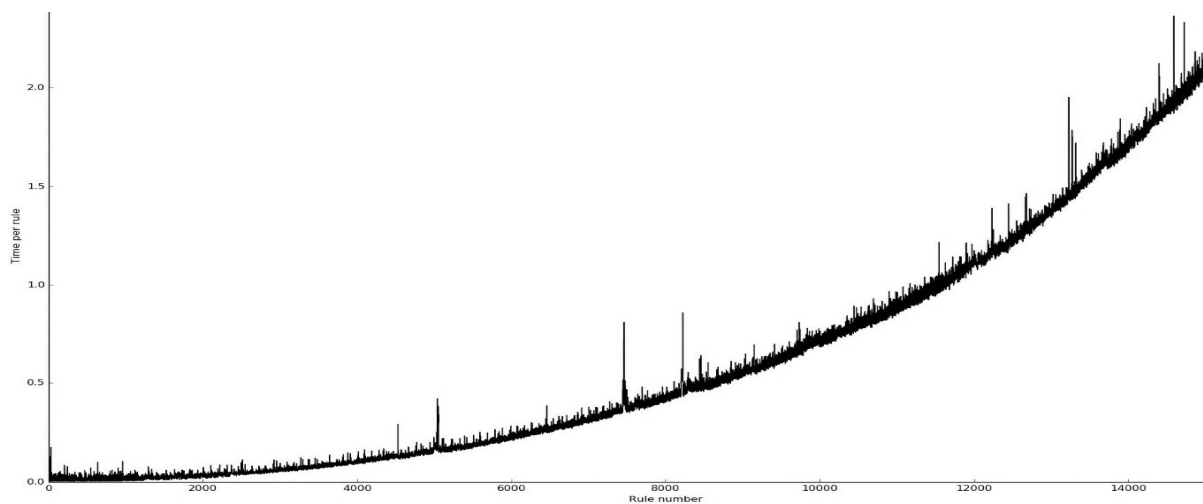


Fig 1. Adding rules to the Floodlight SDN controller through PreFirewall

The growth rate is polynomial due to the algorithm complexity [2]. Table 1 provides more detailed test results:

Taking into account the results obtained in Table 1 and analyzing possible ways of reducing the time the network application used to process a new rule, it was decided to optimize the algorithm used in PreFirewall.

Table 1. Test results

	Floodlight, s	PreFirewall Floodlight, s +
The average time of adding a new rule	0.0115	0.6333
Standard deviation	0.0073	0.6491
Total time taken to process 15 000 rules	172.055	9499.8394
The time taken to add the first rule	0,01	0,04
Rules were added (out of 15 000)	14781	11631

1. Analysis of data structures for a new algorithm

Analysis of the algorithm used in the network application PreFirewall showed that the main problem of low performance is the data structure used to store the rules. A two-dimensional array was used as the repository of rules. As a result of this, the operation of adding a new rule (one of the most frequent operations) became very slow. In the worst case, if the new rule is "good" (adding it does not cause anomalies), it should be compared with all stored rules. Thus, the addition of "good" rules is more complex than the addition of "bad" rules. Taking into account that "good" rules are added more often than "bad" rules, in order to optimize the algorithm, first of all, it is necessary to make the operation of adding "good" rules as simple as possible in terms of complexity. It is worth noting that, without introducing fundamental changes to the algorithm itself, you can achieve the task only if you store the processed rules in the form of a tree. The use of dictionaries, hash tables or databases will not yield any gain, since they are not fundamentally different from a two-dimensional array in their structure.

Table 2. Floodlight firewall rule fields

Filed name	Possible value	Description
switchid	xx:xx:xx:xx:xx:xx:xx:xx	Switch identification number
src-inport	short	Input switch port number
src-mac	xx:xx:xx:xx:xx:xx	Source MAC-address
dst-mac	xx:xx:xx:xx:xx:xx	Destination MAC-address MAC-адрес получателя
dl-type	ARP or IPv4	Protocol
src-ip	A.B.C.D/M	Source IP-address
dst-ip	A.B.C.D/M	Destination IP-address
nw-proto	TCP or UDP or ICMP	Protocol
tp-src	short	Source port number
tp-dst	short	Destination port number
priority	int	Priority of the rule (less is more important)
action	allow or deny	Allow or deny set of network flows which are match rule

So, let us take a closer look at how to introduce security policy rules in the form of a tree. Concerning OpenFlow Standard 1.0, the packet headers have 12 fields [3] (Table 2). Let us arrange the rule fields by the number of possible values that can be contained in them, in ascending order. The field priority and action will be placed at the end of this sequence, since these fields are related to the action of the rule. Thereby, the rules

tree will have a height equals to 12. We establish a one-to-one correspondence between the levels of the tree and the rules fields in such a way that the smaller the number of possible values of the field, the lower the tree level corresponding to it. Thus, we establish a one-to-one correspondence between each rule of security policy that does not contain any anomalies and tree path started at the root and ended in the leaf.

Let each vertex of the tree contain hash table (key-value pair). The key value will be the value of the rule field. The value is the address of the corresponding vertex on the level below. At level 12 of this tree, there will be leaves corresponding to action field and containing two possible values – allow or deny as keys, and the values will be nullptr. A simplified tree model is shown in Fig. 2. This tree will be called a police tree. Nodes marked with a dashed line are not included in the policy tree and are inserted into the scheme only for numbering the rules.

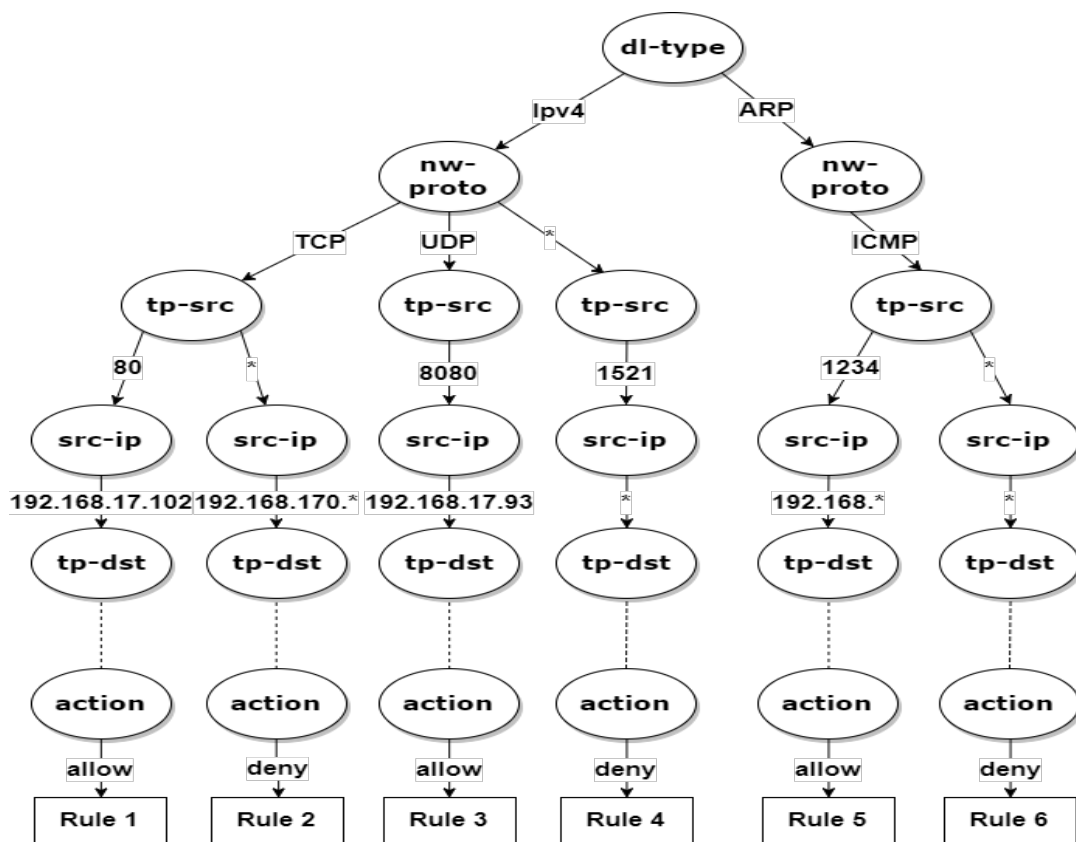


Fig 2. Policy tree example

2. Bulding police tree. Anomalies detection and resolution algorithm

Consider the algorithm for building this tree and finding anomalies among the security policy rules. The algorithm for adding a new rule to a tree is as follows:

- Discovery routine. The DiscoverAnomaly algorithm called. At this stage, it is determined whether the set of security policy rules will remain free of any anomalies,

after addition of the new rule. If so, go to stage 2, otherwise – the completion of the algorithm and showing the anomaly detection message.

- Rule insertion routine. The InsertRule algorithm called. Inserting the rule into the tree and completing the algorithm. Showing message about the insertion of the rule.

The DiscoveryRoutine algorithm is extremely simple. Each field of the new rule is compared with every field of the rules already added in the policy tree, in order to search for anomalies. Anomalies are sought on the basis of their definitions obtained earlier [2].

The decision routine is activated once all the rule fields have been checked and the action field is reached. At that point, the final anomaly state is determined and reported. If the rule action coincides with the action of another rule, an anomaly is discovered. Correlation and generalization are confirmed if the rule actions are different. If the input anomaly state is a generalization and the actions are the same, the existing rule is redundant to the new rule. Finally, if the new rule is a subset or equal to the existing rule, the new rule is redundant if their actions are the same, and is shadowed if their actions are different. If an anomaly is discovered and decided, the user is reported with the type of anomaly and the rules involved.

Thus, to determine the type of anomaly or to make sure that there are no any anomalies, it is required to check the presence of a specific value in hash table on each of the 12 levels of the policy tree. The complexity of this operation is $O(1)$ [4]. Hence, the complexity of the DiscoverAnomaly algorithm is also $O(1)$.

The InsertRule function inserts rules to the policy tree that have been tested by the DiscoverAnomaly function. The complexity of this operation is $O(1)$.

Thus, the proposed modification of the algorithm for determining anomalies have a constant time complexity.

3. Conclusion

Often, network administrators have to modify existing security policy rules, which can lead to anomalies or opening security holes. The detection of anomalies in this case becomes more difficult than detection anomalies while adding new rules, because changing the rule can potentially lead to serious changes in the policy tree as a whole. Effective restructuring of the tree, combining the rearrangement of the old rules, is a complex task. In the future, it is planned to conduct research on the development of effective algorithms for restructuring the policy tree in the case of editing existing rules, as well as carrying out stress testing of the proposed algorithm.

References

- [1] *Floodlight SDN OpenFlow Controller*, <https://github.com/floodlight/floodlight>.
- [2] Morzhov S., Alekseev I., Nikitinskiy M., “Firewall application for Floodlight SDN controller”, International Siberian Conference on Control and Communications (SIBCON) (12–14 May, 2016, Moscow, Russia), 1–5.
- [3] *OpenFlow Switch Specification, Version 1.4.0*, <http://networkstatic.net/wp-content/uploads/2013/10/openflow-spec-v1.4.0.pdf>.

- [4] Cormen T., Leiserson C., Rivest R., Stein C., *Introduction to Algorithms*, 3rd., Massachusetts Institute of Technology Press, 2009, ISBN: 978-0-262-03384-8.

Моржов С. В., Никитинский М. А., "Новый подход к обнаружению и устранению аномалий в политике безопасности внешнего модуля межсетевого экрана контроллера ПКС Floodlight", *Моделирование и анализ информационных систем*, 25:3 (2018), 251–256.

DOI: 10.18255/1818-1015-2018-3-251-256

Аннотация. Авторы рассматривают разработанное сетевое приложение PreFirewall для контроллера *программно-конфигурируемой сети* (ПКС) Floodlight. Данное сетевое приложение осуществляет фильтрацию устанавливаемых правил в модуль ядра firewall контроллера Floodlight с целью недопущения возникновения аномалий между устанавливаемыми правилами. Разработанное сетевое приложение PreFirewall прошло ряд тестов. В результате проведенного нагрузочного тестирования было установлено, что время добавления новых правил, при использовании PreFirewall, серьезно возрастает с ростом количества ранее обработанных правил. Анализ сетевого приложения PreFirewall показал, что при добавлении правила (самая частая операция), в худшем случае необходимо произвести его сравнение со всеми существующими правилами, которые хранятся в виде двумерного массива. Таким образом, операция добавления нового правила является наиболее трудоемкой и сильнее всего влияет на производительность сетевого приложения, что приводит к возрастанию времени его отклика. Одним из возможных путей решения данной проблемы является выбор такой структуры данных, используемой для хранения правил, в которой операция добавления нового правила была бы простой. В качестве такой структуры предлагается использование дерева, каждая вершина которого содержит всевозможные значения полей в устанавливаемых правилах. Данный подход обеспечивает константную сложность операции добавления нового правила и, следовательно, решает проблему производительности сетевого приложения PreFirewall. Статья публикуется в авторской редакции.

Ключевые слова: межсетевой экран, Floodlight, хеш-таблица, сетевой контроллер, дерево правил, PreFirewall, разрешение возникающих аномалий, ПКС, программно-конфигурируемая сеть

Об авторах:

Моржов Сергей Владимирович, orcid.org/0000-0001-6652-3574, магистрант,
Ярославский государственный университет им. П.Г. Демидова,
ул. Советская, 14, г. Ярославль, 150003 Россия, e-mail: smorzhov@gmail.com

Никитинский Михаил Александрович, orcid.org/0000-0001-8830-8613, программист-аналитик,
ООО «Энергия-Инфо», ул. Союзная, 144, г. Ярославль, 150008 Россия, e-mail: man@a-real.ru

Благодарности:

¹Работа выполнена при финансовой поддержке РФФИ, проект № 16-07-01103а.

Вероятностные модели

©Родина Л. И., Тютеев И.И., 2018

DOI: 10.18255/1818-1015-2018-3-257-267

УДК 517.935

Об оценке средней временной выгоды в вероятностных эколого-экономических моделях

Родина Л. И.¹, Тютеев И.И.

получена 12 марта 2018

Аннотация. Рассматриваются эколого-экономические модели оптимального сбора ресурса, заданные дифференциальными уравнениями с импульсным воздействием, которые зависят от случайных параметров. Предполагаем, что длины интервалов θ_k между моментами импульсов τ_k являются случайными величинами и размеры импульсного воздействия зависят от случайных параметров v_k , $k = 1, 2, \dots$. Одним из примеров таких объектов является уравнение с импульсами, моделирующее динамику популяции, подверженной промыслу. При отсутствии эксплуатации развитие популяции описывается дифференциальным уравнением $\dot{x} = g(x)$, а в моменты времени τ_k из популяции извлекается случайная доля ресурса v_k , $k = 1, 2, \dots$. На процесс сбора можно влиять таким образом, чтобы остановить заготовку в том случае, когда ее доля окажется достаточно большой, чтобы сохранить возможно больший остаток ресурса для увеличения размера следующего сбора. Пусть уравнение $\dot{x} = g(x)$ имеет асимптотически устойчивое решение $\varphi(t) \equiv K$, областью притяжения которого является интервал (K_1, K_2) , где $0 \leq K_1 < K < K_2$. Построено управление $u = (u_1, \dots, u_k, \dots)$, ограничивающее долю добываемого ресурса в каждый момент времени τ_k таким образом, чтобы количество оставшегося ресурса, начиная с некоторого момента τ_{k_0} , было не меньше заданного значения $x \in (K_1, K)$. Для любого $x \in (K_1, K)$ получены оценки средней временной выгоды, выполненные с вероятностью единица. Показано, что существует единственное $x^* \in (K_1, K)$, при котором оценка снизу достигает наибольшего значения. Таким образом, описан способ эксплуатации популяции, при котором значение средней временной выгоды можно оценить снизу с вероятностью единица по возможности наибольшим числом.

Ключевые слова: модель популяции, подверженной промыслу, средняя временная выгода, оптимальная эксплуатация

Для цитирования: Родина Л. И., Тютеев И.И., "Об оценке средней временной выгоды в вероятностных эколого-экономических моделях", *Моделирование и анализ информационных систем*, **25:3** (2018), 257–267.

Об авторах:

Родина Людмила Ивановна, orcid.org/0000-0003-1077-2189, д-р физ.-мат. наук, профессор кафедры функционального анализа и его приложений, Владимирский государственный университет им. А.Г. и Н.Г. Столетовых ул. Горького, 87, Владимир, 600000 Россия, e-mail: LRodina67@mail.ru

Тютеев Илья Индусович, orcid.org/0000-0002-3850-2781, аспирант, Удмуртский государственный университет, ул. Университетская, 1, Ижевск, 426034 Россия, e-mail: it.30@mail.ru

Благодарности:

¹ Работа выполнена при финансовой поддержке РФФИ (проект № 16–01–00346–а).

Введение

Рассматриваются эколого-экономические модели оптимального сбора ресурса, заданные дифференциальными уравнениями с импульсным воздействием, которые зависят от случайных параметров. Предполагаем, что длины интервалов $\theta_k = \tau_k - \tau_{k-1}$ между моментами импульсов τ_k являются случайными величинами и размеры импульсного воздействия зависят от случайных параметров v_k , $k = 1, 2, \dots$. Одним из примеров таких объектов является уравнение с импульсами, моделирующее динамику популяции, подверженной промыслу; полагаем, что изменение размера популяции (равное размеру промысловых заготовок) в моменты τ_k , а также сами эти моменты зависят от различных воздействий внешней среды, поэтому динамика популяции описывается уравнением со случайными параметрами. При отсутствии эксплуатации развитие популяции описывается дифференциальным уравнением $\dot{x} = g(x)$, а в моменты времени τ_k из популяции извлекается некоторая случайная доля ресурса v_k , $k = 1, 2, \dots$. Здесь $\theta_k \in \Omega_1 \subseteq [\alpha_1, \beta_1]$, где $0 < \alpha_1 \leq \beta_1 < \infty$, $v_k \in \Omega_2 \subseteq [0, 1]$.

Пусть имеется возможность влиять на процесс сбора ресурса таким образом, чтобы остановить заготовку в том случае, когда ее доля окажется достаточно большой (больше некоторого значения $u_k \in [0, 1)$ в момент τ_k), чтобы сохранить возможно больший остаток ресурса для увеличения размера следующего сбора. В этом случае доля добываемого ресурса будет равна $\ell_k = \ell(v_k, u_k)$, где

$$\ell(v_k, u_k) = \begin{cases} v_k, & \text{если } v_k < u_k, \\ u_k, & \text{если } v_k \geq u_k. \end{cases}$$

Таким образом, мы рассматриваем эксплуатируемую популяцию, динамика которой задана дифференциальным уравнением с импульсным воздействием

$$\begin{aligned} \dot{x} &= g(x), \quad t \neq \tau_k, \\ \Delta x|_{t=\tau_k} &= -\ell(v_k, u_k)x, \quad k = 1, 2, \dots, \end{aligned} \quad (1)$$

где $\Delta x|_{t=\tau_k} = x(\tau_k) - x(\tau_k - 0)$, $\theta_k = \tau_k - \tau_{k-1} \in \Omega_1$, $(x, v_k, u_k) \in [0, +\infty) \times \Omega_2 \times [0, 1]$. Предполагаем, что решения уравнения непрерывны справа, функция $g(x)$ определена и непрерывно дифференцируема для всех $x \in [0, +\infty)$. Пусть также имеет место следующее условие — *существует $K > 0$ такое, что $\varphi(t) \equiv K$ является асимптотически устойчивым решением уравнения $\dot{x} = g(x)$* . Данное условие выполнено, если $K > 0$ — стационарное состояние уравнения $\dot{x} = g(x)$ и $g'(K) < 0$ (см. [1, с. 30]). В частности, оно выполнено для следующих уравнений:

1. Логистическое уравнение $\dot{x} = (a - bx)x$, где коэффициенты $a > 0$ и $b > 0$ являются показателями роста популяции и внутривидовой конкуренции соответственно. Этим уравнением также описывается эффективность рекламного воздействия на покупателей при реализации нового товара.

2. Уравнение, учитывающее нижнюю критическую границу численности популяции и самоограничение при больших плотностях $\dot{x} = a \frac{\beta x^2}{\beta + \gamma x} - dx - \delta x^2$; здесь все постоянные $a, \beta, \gamma, d, \delta$ положительные (модель динамики популяции А.Д. Базикина, см. [1, с. 44]).

3. Уравнение динамики популяции $\dot{x} = ax(x - L)(K - x)$, где $a > 0$, $K > L > 0$, L — нижняя критическая плотность популяции, K — стационарная плотность.

4. Уравнение Гомпертца $\dot{x} = -\frac{\varepsilon x}{\ln K} \ln \frac{x}{K}$, где $\varepsilon > 0$, $K > 1$.

Обозначим $U \doteq \{u : u = (u_1, \dots, u_k, \dots)\}$, где $u_k \in [0, 1]$, $\theta \doteq (\theta_1, \dots, \theta_k, \dots)$, $\theta_k \in \Omega_1$, $\ell \doteq (\ell_1, \dots, \ell_k, \dots)$, $\ell_k = \ell(v_k, u_k)$. Пусть $X_k = X_k(\theta, \ell, x_0)$ — количество ресурса до сбора в момент τ_k , $k = 1, 2, \dots$, зависящее от длин промежутков $\theta_1, \dots, \theta_k$ между моментами сбора, долей ресурса $\ell_i = \ell(v_i, u_i)$, $i = 1, \dots, k - 1$, собранного в предыдущие моменты времени, и начального значения x_0 . Для любого $x_0 \geq 0$ введем в рассмотрение функцию

$$H_*(\theta, \ell, x_0) \doteq \lim_{n \rightarrow \infty} \frac{\sum_{k=1}^n X_k(\theta, \ell, x_0) \ell_k}{\sum_{k=1}^n \theta_k}, \quad (2)$$

которую назовем *средней временной выгодой* от извлечения ресурса.

Предположим, что областью притяжения решения $\varphi(t) \equiv K$ является интервал (K_1, K_2) , где $0 \leq K_1 < K < K_2$. В данной работе построено управление $u = (u_1, \dots, u_k, \dots)$, ограничивающее долю добываемого ресурса в каждый момент времени τ_k таким образом, чтобы количество оставшегося ресурса, начиная с некоторого момента τ_{k_0} (зависящего от x_0), было не меньше заданного значения $x \in (K_1, K)$. Для любого $x \in (K_1, K)$ получены оценки средней временной выгоды, выполненные с вероятностью единица. Показано, что существует единственное $x^* \in (K_1, K)$, при котором оценка снизу достигает наибольшего значения. Таким образом, мы описываем способ эксплуатации популяции, при котором значение средней временной выгоды $H_*(\theta, \ell, x_0)$ можно оценить снизу с вероятностью единица по возможности наибольшим числом.

Отметим, что в детерминированном случае, когда длины промежутков между импульсами и величины импульсного воздействия фиксированы, различные задачи оптимальной эксплуатации популяций исследуются в [2–5]. Одной из первых работ, посвященной оптимальному сбору ресурса в вероятностных моделях, является, по-видимому, [6], в которой показано, что стохастическую рыбную популяцию можно эксплуатировать до достижения определенного уровня (escapement level), не зависящего от текущего размера популяции. Сравнение различных характеристик для вероятностной и детерминированной моделей проводится в [6, 7]; вопросы оптимальной эксплуатации популяций, заданных различными вероятностными моделями, также рассматриваются в [8–10] (более подробный обзор литературы приведен в [7]). В работе [11] получены оценки функции $H_*(\theta, \ell, x_0)$ в случае, когда динамика популяции задана логистическим уравнением $\dot{x} = (a - bx)x$ и длины промежутков между импульсами одинаковые. Здесь также показано, что при недостаточном ограничении на извлечение ресурса значение средней временной выгоды (2) может равняться нулю для всех или для почти всех значений случайных параметров.

1. Описание вероятностной модели

Вероятностная модель, заданная дифференциальным уравнением со случайными параметрами (1), подробно описана в работах [12, 13]. Приведем краткое описание для полноты изложения. В данной модели моменты τ_k являются моментами скачков для системы с импульсным воздействием; в частном случае, $\tau_1, \tau_2, \dots$ — это моменты промысловых заготовок для модели популяции, подверженной промыслу. Полагаем, что $\tau_0 = 0$, $\theta_k = \tau_k - \tau_{k-1} \in \Omega_1 \subseteq [\alpha_1, \beta_1]$ и величина скачка в момент τ_k зависит от случайного параметра $v_k \in \Omega_2 \subseteq [0, 1]$. Таким образом, все параметры принадлежат множеству $\Omega = \Omega_1 \times \Omega_2$, причем любое из множеств Ω_1 или Ω_2 может содержать только один элемент. Если все множество Ω состоит из одного элемента, вероятностная модель совпадает с детерминированной.

Определим вероятностное пространство $(\Sigma, \mathfrak{A}, \mu)$ как прямое произведение вероятностных пространств $(\Sigma_1, \mathfrak{A}_1, \mu_1)$ и $(\Sigma_2, \mathfrak{A}_2, \mu_2)$. Здесь Σ_1 означает множество числовых последовательностей $\theta = (\theta_0, \theta_1, \dots, \theta_k, \dots)$, где $\theta_k \in \Omega_1$, система множеств $\mathfrak{A}_1$ является наименьшей сигма-алгеброй, порожденной цилиндрическими множествами

$$E_k \doteq \{\theta \in \Sigma_1 : \theta_1 \in I_1, \dots, \theta_k \in I_k\}, \quad \text{где } I_i \doteq (t_i, s_i], \quad i = 1, \dots, k,$$

а вероятностная мера μ_1 определена следующим образом. Для каждого промежутка I_i , $i = 1, 2, \dots$, определим вероятностную меру $\tilde{\mu}_1(I_i) = F_1(s_i) - F_1(t_i)$ с помощью функции распределения $F_1(t)$. На алгебре цилиндрических множеств построим меру

$$\tilde{\mu}_1(E_k) = \tilde{\mu}_1(I_1) \cdot \dots \cdot \tilde{\mu}_1(I_k),$$

тогда в силу теоремы А. Н. Колмогорова (см., например, [14, с. 176]) на измеримом пространстве $(\Sigma_1, \mathfrak{A}_1)$ существует единственная вероятностная мера μ_1 , которая является продолжением меры $\tilde{\mu}_1$ на сигма-алгебру $\mathfrak{A}_1$. Таким же образом определяем вероятностное пространство $(\Sigma_2, \mathfrak{A}_2, \mu_2)$, где $\Sigma_2 \doteq \{v : v = (v_1, \dots, v_k, \dots)\}$, $v_k \in \Omega_2$, мера $\tilde{\mu}_2$ задана с помощью функции распределения $F_2(t)$.

Отметим, что $\Sigma = \Sigma_1 \times \Sigma_2 = \{\sigma : \sigma = (\omega_1, \dots, \omega_k, \dots)\}$, где $\omega_k = (\theta_k, v_k) \in \Omega$. Зададим сигма-алгебру $\mathfrak{A} = \mathfrak{A}_1 \times \mathfrak{A}_2$ и меру $\mu = \mu_1 \times \mu_2$, которая является прямым произведением вероятностных мер μ_1 и μ_2 . Это означает, что $\mu(A \times B) = \mu_1(A)\mu_2(B)$ для всех $A \in \mathfrak{A}_1$, $B \in \mathfrak{A}_2$.

2. Оценка средней временной выгоды для вероятностной модели динамики популяции

Определим $\varphi(t, x)$ как решение уравнения $\dot{x} = g(x)$, удовлетворяющее начальному условию $\varphi(0, x) = x$, где $t \geq 0$, $x \geq 0$. Если $\vartheta \in \Omega_1$, то функция $\varphi(\vartheta, x)$ является случайной величиной, заданной на множестве Ω_1 . Положим $u(x, \varphi(\vartheta, x)) = 1 - \frac{x}{\varphi(\vartheta, x)}$.

Рассмотрим функцию

$$\ell(\omega, x) = \ell(v, u(x, \varphi(\vartheta, x))) = \begin{cases} v, & \text{если } v < u(x, \varphi(\vartheta, x)), \\ u(x, \varphi(\vartheta, x)), & \text{если } v \geq u(x, \varphi(\vartheta, x)), \end{cases} \quad (3)$$

которая является случайной величиной на множестве $\Omega = \Omega_1 \times \Omega_2$.

Если $g(K) = 0$, то уравнение $\dot{x} = g(x)$ имеет решение $\varphi(t) \equiv K$. Если $g'(K) < 0$, то решение $\varphi(t) \equiv K$ асимптотически устойчиво. Напомним, что областью асимптотической устойчивости (областью притяжения) решения $\varphi(t) \equiv K$ уравнения $\dot{x} = g(x)$ является множество всех точек $x \in \mathbb{R}$, обладающих свойством $\lim_{t \rightarrow \infty} \varphi(t, x) = K$.

Буквой M будем обозначать математическое ожидание случайной величины, m_θ — математическое ожидание длин интервалов $\theta_1, \theta_2, \dots$. Отметим, что $0 < \alpha_1 \leq m_\theta \leq \beta_1 < \infty$.

Теорема 1. Пусть выполнены следующие условия:

1) уравнение $\dot{x} = g(x)$ имеет асимптотически устойчивое решение $\varphi(t) \equiv K$ и интервал (K_1, K_2) является областью притяжения этого решения ($0 \leq K_1 < K < K_2$);

2) $\Omega_1 \subseteq [\alpha_1, \beta_1]$, где $0 < \alpha_1 \leq \beta_1 < \infty$, $\Omega_2 \subseteq [0, 1]$ и $F_2(0) < 1$.

Тогда для любых $(x, x_0) \in (K_1, K) \times (K_1, K_2)$ существует управление $u \in U$ такое, что для почти всех $\sigma \in \Sigma$ выполнены неравенства

$$\frac{M(\varphi(\vartheta, x)\ell(\omega, x))}{m_\theta} \leq H_*(\theta, \ell, x_0) \leq \frac{KM\ell(\omega, x)}{m_\theta}. \quad (4)$$

Доказательство. Пусть X_k — размер популяции перед и x_k — размер популяции после извлечения ресурса в некоторый момент времени τ_k ; тогда $x_k = (1 - \ell_k)X_k$, $k = 1, 2, \dots$. Покажем, что управления u_k , при которых выполнено (4), можно определить равенствами $u_k = 1 - \frac{x}{\varphi(\theta_k, x)}$ при всех $k > k_0$, где k_0 зависит от начального размера популяции x_0 . Рассмотрим три случая.

1. Если $x_0 \in [x, K]$, то $X_1 = \varphi(\theta_1, x_0) \geq \varphi(\theta_1, x)$. Поскольку (K_1, K_2) является областью притяжения решения $\varphi(t) \equiv K$, то функция $t \mapsto \varphi(t, x)$ возрастает для любого $x \in (K_1, K)$, поэтому $\varphi(t, x) > \varphi(0, x) = x$ для всех $t > 0$, $x \in (K_1, K)$. Положим $u_k = 1 - \frac{x}{\varphi(\theta_k, x)}$ для всех $k \in \mathbb{N}$, тогда из неравенства $\ell_1 \leq u_1$ следует, что

$$x_1 = (1 - \ell_1)X_1 \geq (1 - u_1)X_1 = \frac{xX_1}{\varphi(\theta_1, x)} \geq x.$$

Далее, $X_2 = \varphi(\theta_2, x_1) \geq \varphi(\theta_2, x)$. Аналогично получаем, что $X_k \geq \varphi(\theta_k, x)$ для всех $k \in \mathbb{N}$. Поэтому, если $u = (u_1, \dots, u_k, \dots)$, то $\ell_k = \ell(\omega_k, x)$ и

$$H_*(\theta, \ell, x_0) \geq \lim_{n \rightarrow \infty} \frac{1}{\sum_{k=1}^n \theta_k} \sum_{k=1}^n \varphi(\theta_k, x)\ell(\omega_k, x). \quad (5)$$

2. Пусть $x_0 \in (K_1, x)$. Положим $u_k = 0$ для всех $k = 1, \dots, k_0$, где $k_0 = k_0(x_0)$ — первое из натуральных чисел, таких что $x_k = X_k = \varphi(\tau_k, x_0) \geq x$. Данное значение k_0 существует, так как точка x_0 содержится в области притяжения решения $\varphi(t) \equiv K$. Определим $u_k = 1 - \frac{x}{\varphi(\theta_k, x)}$ для всех $k > k_0$, тогда $X_k \geq \varphi(\theta_k, x)$ при всех $k > k_0$; это доказывается так же, как в первом пункте. Следовательно, неравенство (5) справедливо при выбранном управлении $u = (u_1, \dots, u_k, \dots)$.

Отметим, что случайные величины $\varphi(\theta_k, x)\ell(\omega_k, x)$ независимы, одинаково распределены и так как $0 \leq \varphi(\theta_k, x)\ell(\omega_k, x) < Ku(x, \varphi(\theta_k, x))$ для всех $k \in \mathbb{N}$, то

$$M|\varphi(\theta_k, x)\ell(\omega_k, x)| < KM u(x, \varphi(\theta_k, x)) \leq K < \infty.$$

Тогда из усиленного закона больших чисел Колмогорова следует, что для почти всех $\sigma \in \Sigma$ имеет место равенство

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^n \varphi(\theta_k, x)\ell(\omega_k, x) = M(\varphi(\vartheta, x)\ell(\omega, x)).$$

Из усиленного закона больших чисел также следует, что $\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^n \theta_k = m_\theta$, поэтому из (5) получаем первое неравенство в (4).

Далее, если $x_0 \leq K$, то $X_k \leq K$ для любых u_k и всех $k \in \mathbb{N}$, поэтому

$$H_*(\theta, \ell, x_0) \leq K \lim_{n \rightarrow \infty} \frac{1}{\sum_{k=1}^n \theta_k} \sum_{k=1}^n \ell(\omega_k, x) = \frac{KM\ell(\omega, x)}{m_\theta}$$

для почти всех $\sigma \in \Sigma$, то есть выполнено последнее неравенство в (4).

3. Покажем, что утверждение теоремы справедливо при $x_0 \in (K, K_2)$. Пусть $k_1 = k_1(x_0)$ — наименьшее из натуральных чисел, таких что $x_k \leq K$ при $u_1 = \dots = u_k = 1$; покажем, что данное число существует с вероятностью единица. Отметим сначала, что такое число существует, если $v_{k_1} = 1$ при некотором $k_1 \in \mathbb{N}$; тогда $x_k = 0$ при всех $k \geq k_1$.

Пусть теперь $v_k \neq 1$ для всех $k \in \mathbb{N}$. Поскольку функция $t \mapsto \varphi(t, x)$ монотонно убывает при $x > K$, то $X_{k+1} = \varphi(\theta_{k+1}, x_k) < x_k$, если $x_k > K$, $k = 0, 1, \dots$. Далее, если $u_k = 1$, то $\ell(v_k, 1) = v_k$; поэтому, если $x_0 > K$ и $u_1 = 1$, то $x_1 = X_1(1 - v_1) < x_0(1 - v_1)$; если $x_1 > K$ и $u_1 = u_2 = 1$, то

$$x_2 = X_2(1 - v_2) < x_1(1 - v_2) < x_0(1 - v_1)(1 - v_2).$$

Аналогично получаем, что если $x_k > K$ и $u_1 = \dots = u_{k+1} = 1$, то

$$x_{k+1} < x_0(1 - v_1)(1 - v_2) \cdot \dots \cdot (1 - v_{k+1}).$$

Рассмотрим последовательность независимых одинаково распределенных случайных величин $\{C_k(v)\}_{k=1}^\infty$, где $C_k(v) = C_k(v_k) = 1 - v_k$. Введем также последовательность $\{S_k(v)\}_{k=1}^\infty$, где

$$S_k(v) = \ln(1 - v_1) + \dots + \ln(1 - v_k),$$

которая является случайным блужданием на прямой. Покажем, что если $F_2(0) < 1$, то

$$M \ln(1 - v_k) < 0. \quad (6)$$

Действительно, так как $v_k \in [0, 1)$, то $\ln(1 - v_k) \leq 0$, поэтому для математического ожидания либо выполнено неравенство (6), либо $M \ln(1 - v_k) = 0$. В последнем

случае $v_k = 0$ с вероятностью единица [14, глава 2, §6], что противоречит условию $F_2(0) = \tilde{\mu}_2(v_k = 0) < 1$. Из (6) следует, что с вероятностью единица $S_k(v)$ уходит в минус бесконечность (см. [15, глава 12, §2]). Это означает, что существует множество $\Sigma_2^0 \subseteq \Sigma_2$ такое, что $\mu_2(\Sigma_2^0) = 1$ и $\lim_{k \rightarrow \infty} S_k(v) = -\infty$ для всех $v \in \Sigma_2^0$. Следовательно, $\lim_{k \rightarrow \infty} C_1(v_1) \cdot \dots \cdot C_k(v_k) = 0$ для всех $v \in \Sigma_2^0$, поэтому с вероятностью единица найдется $k_1 = k_1(x_0)$ такое, что $X_{k_1}(1 - v_{k_1}) \leq K$.

Выберем управление $u_k = 1$ для всех $k = 1, \dots, k_1 - 1$, $u_{k_1} = 1 - \frac{x}{X_{k_1}}$ и $u_k = 1 - \frac{x}{\varphi(\theta_k, x)}$ для всех $k > k_1$. Тогда из $x_{k_1} = X_{k_1}(1 - \ell_{k_1})$ и неравенства $v_k \leq \ell(v_k, u_k) \leq u_k$ получаем, что

$$x = X_{k_1}(1 - u_{k_1}) \leq x_{k_1} \leq X_{k_1}(1 - v_{k_1}) \leq K.$$

Дальнейшее доказательство повторяет доказательство первых двух пунктов. $\square$

3. Построение наибольшей оценки снизу для средней временной выгоды, выполненной с вероятностью единица

Из равенства (3) следует, что

$$\varphi(\vartheta, x)\ell(\omega, x) = \begin{cases} v\varphi(\vartheta, x), & \text{если } v < u(x, \varphi(\vartheta, x)), \\ \varphi(\vartheta, x) - x, & \text{если } v \geq u(x, \varphi(\vartheta, x)). \end{cases}$$

Предположим, что распределения F_1 и F_2 имеют плотности f_1 и f_2 соответственно. Рассмотрим математическое ожидание случайной величины $\varphi(\vartheta, x)\ell(\omega, x)$ как функцию переменной x :

$$m(x) \doteq M(\varphi(\vartheta, x)\ell(\omega, x)) = \int_0^\infty \varphi(t, x)f_1(t)dt \int_0^{u(x, \varphi(t, x))} sf_2(s)ds + \\ + \int_0^\infty (\varphi(t, x) - x) \left(1 - F_2(u(x, \varphi(t, x)))\right) f_1(t)dt. \quad (7)$$

Утверждение 1. Пусть распределения F_1 и F_2 имеют плотности f_1 и f_2 соответственно, $g(K_1) = g(K) = 0$, $g'(K) < 0$, $g'(K_1) > 0$, $g''(x) < 0$ при $x \in (K_1, K)$. Тогда функция $m(x)$ достигает максимального значения при $x = x^*$, где $x^* \in (K_1, K)$ является единственным решением уравнения $m'(x) = 0$:

$$\int_0^\infty \varphi'_x(t, x)f_1(t)dt \int_0^{u(x, \varphi(t, x))} sf_2(s)ds + \int_0^\infty (\varphi'_x(t, x) - 1) \left(1 - F_2(u(x, \varphi(t, x)))\right) f_1(t)dt = 0. \quad (8)$$

Доказательство. Напомним, что через $\varphi(t, x)$ мы обозначаем решение уравнения $\dot{x} = g(x)$, удовлетворяющее начальному условию $\varphi(0, x) = x$. Покажем, что неравенства $\varphi'_x(t, x) \geq 0$ и $\varphi''_{xx}(t, x) \leq 0$ выполнены для всех $(t, x) \in (0, \infty) \times (K_1, K)$.

Из единственности решений уравнения следует, что функция $x \mapsto \varphi(t, x)$ возрастающая. Действительно, если существуют такие $x_1 < x_2$, что $\varphi(t, x_1) \geq \varphi(t, x_2)$, то найдется точка $t_* \in (0, t]$ такая, что $\varphi(t_*, x_1) = \varphi(t_*, x_2)$; получили противоречие.

Рассмотрим функцию $\psi(t, x) \doteq \varphi'_x(t, x)$, которая удовлетворяет уравнению $\dot{y} = g'_x(\varphi(t, x))y$ и начальному условию $\psi(0, x) = 1$ для всех $x \in [K_1, K]$ (см. [16, глава 5, §23]). Так как $g''(x) < 0$ при $x \in (K_1, K)$, то $g'(x)$ убывает на данном интервале. Функция $x \mapsto \varphi(t, x)$ возрастающая, поэтому $x \mapsto g'_x(\varphi(t, x))$ убывает для любого фиксированного $t \in (0, \infty)$. Таким образом, если $x_1 < x_2$, то

$$g'_x(\varphi(t, x_1)) > g'_x(\varphi(t, x_2))$$

при каждом $t \in (0, \infty)$. Поэтому в силу теоремы Чаплыгина о дифференциальном неравенстве (см. [17]) $\psi(t, x_1) > \psi(t, x_2)$, то есть $\varphi'_x(t, x_1) > \varphi'_x(t, x_2)$ для любого $t \in (0, \infty)$. Это означает, что функция $x \mapsto \varphi'_x(t, x)$ убывающая, тогда $\varphi''_{xx}(t, x) \leq 0$ для всех $(t, x) \in (0, \infty) \times (K_1, K)$, причем множество тех $x \in (K_1, K)$, при которых $\varphi''_{xx}(t, x) = 0$, не более чем счетно.

Чтобы показать, что (8) имеет единственное решение, нужно доказать, что функция $m'(x)$ убывает на интервале (K_1, K) и на концах интервала удовлетворяет неравенствам $m'(K_1) > 0$, $m'(K) < 0$. Найдем

$$\begin{aligned} m''(x) = \int_0^\infty \varphi''_{xx}(t, x) f_1(t) dt \int_0^{u(x, \varphi(t, x))} s f_2(s) ds + \\ + \int_0^\infty \varphi''_{xx}(t, x) \left(1 - F_2(u(x, \varphi(t, x)))\right) f_1(t) dt. \end{aligned}$$

Тогда из условий, полученных для функции $\varphi''_{xx}(t, x)$, следует, что $m''(x) \leq 0$ для всех $x \in (K_1, K)$ и множество тех $x \in (K_1, K)$, при которых $m''(x) = 0$, не более чем счетно; поэтому $m'(x)$ убывает на (K_1, K) . Далее, так как $g(K_1) = g(K) = 0$, то $\varphi(t, K) \equiv K$, $\varphi(t, K_1) \equiv K_1$, поэтому $u(K, \varphi(t, K)) = u(K_1, \varphi(t, K_1)) = 0$; из (8) следует, что

$$m'(K) = (1 - F_2(0)) \int_0^\infty (\varphi'_x(t, K) - 1) f_1(t) dt. \quad (9)$$

Функция $\psi(t, K) \doteq \varphi'_x(t, K)$ удовлетворяет уравнению $\dot{y} = g'(K)y$, где $g'(K) < 0$; поэтому $\psi(t, K)$ является убывающей и, так как $\psi(0, K) = 1$, то $\varphi'_x(t, K) = \psi(t, K) < 1$ для всех $t \in (0, \infty)$. Таким образом, из (9) следует, что $m'(K) < 0$. Аналогично, из неравенства $g'(K_1) > 0$ получаем, что $m'(K_1) > 0$. $\square$

При доказательстве теоремы 1 построено управление $u \in U$ такое, что для любых $(x, x_0) \in (K_1, K) \times (K_1, K_2)$ неравенства (4) выполнены при почти всех $\sigma \in \Sigma$. Пусть математическое ожидание $m(x) = M(\varphi(\vartheta, x)\ell(\omega, x))$ достигает максимального значения при $x = x^* \in (K_1, K)$. В следующем утверждении приведено одно из управлений $u^* = (u_1^*, u_2^*, \dots) \in U$, при котором среднюю временную выгоду $H_*(\theta, \ell, x_0)$ можно оценить снизу по возможности наибольшим числом. Данное управление u^* ограничивает долю добываемого ресурса в каждый момент сбора τ_k таким образом, чтобы количество оставшегося ресурса, начиная с некоторого момента времени $\tau_{k_0}(x_0)$, было не меньше значения x^* . Оно строится по тому же принципу, что и управление $u \in U$ в теореме 1.

Следствие 1. Пусть $m(x)$ достигает максимального значения при $x = x^* \in (K_1, K)$; $\tilde{u}_k^* \doteq 1 - \frac{x^*}{\varphi(\theta_k, x^*)}$, $k \in \mathbb{N}$. Управление $u^* = (u_1^*, u_2^*, \dots) \in U$, при котором для любого $x_0 \in (K_1, K_2)$ при почти всех $\sigma \in \Sigma$ выполнены неравенства

$$\frac{M(\varphi(\vartheta, x^*)\ell(\omega, x^*))}{m_\theta} \leq H_*(\theta, \ell, x_0) \leq \frac{KM\ell(\omega, x^*)}{m_\theta},$$

можно определить следующим образом:

- 1) если $x_0 \in [x^*, K]$, то $u_k^* = \tilde{u}_k^*$ для всех $k \in \mathbb{N}$;
- 2) если $x_0 \in (K_1, x^*)$, то $u_k^* = 0$ для всех $k = 1, \dots, k_0$ и $u_k^* = \tilde{u}_k^*$ для всех $k > k_0$, где $k_0 = k_0(x_0)$ — наименьшее из натуральных чисел, таких что $x_k \geq x^*$ при $u_1 = \dots = u_k = 0$;
- 3) если $x_0 \in (K, K_2)$, то $u_k^* = 1$ для всех $k = 1, \dots, k_1 - 1$, $u_{k_1}^* = 1 - \frac{x^*}{X_{k_1}}$, $u_k^* = \tilde{u}_k^*$ для всех $k > k_1$; здесь $k_1 = k_1(x_0)$ — наименьшее из натуральных чисел, таких что $x_k \leq K$ при $u_1 = \dots = u_k = 1$.

Пример 1. Найдем оценку средней временной выгоды $H_*(\theta, \ell, x_0)$ для уравнения (1), в котором $g(x) = x(1 - x)$; то есть при отсутствии эксплуатации динамика популяции задана логистическим уравнением $\dot{x} = x(1 - x)$. Пусть распределение F_1 длин интервалов $\theta_1, \theta_2, \dots$ между моментами извлечения ресурса является равномерным на отрезке $[1, 2]$, а распределение F_2 величин $v_1, v_2, \dots$ — равномерным на отрезке $[0, 1]$.

Отметим, что решением уравнения $\dot{x} = x(1 - x)$, удовлетворяющим начальному условию $\varphi(0, x) = x$, является функция

$$\varphi(t, x) = \frac{xe^t}{1 - x + xe^t}$$

и, кроме того, данное уравнение имеет асимптотически устойчивое решение $\varphi(t) \equiv 1$. Выпишем математическое ожидание случайной величины $\varphi(\vartheta, x)\ell(\omega, x)$, опуская промежуточные вычисления:

$$\begin{aligned} m(x) &= \int_1^2 \frac{xe^t dt}{1 - x + xe^t} \int_0^{(1-x)(1-e^{-t})} s ds + \int_1^2 x(1-x)(1-e^{-t}) dt = \\ &= \frac{1}{2} \left(\ln(x(e^2 - 1) + 1) - \ln(x(e - 1) + 1) - x^2 + (e^{-2} - e^{-1})x(1-x) \right). \end{aligned}$$

Также найдем

$$\begin{aligned} M\ell(\omega, x) &= \int_1^2 dt \int_0^{(1-x)(1-e^{-t})} s ds + (1-x) \int_1^2 (e^{-t} - e^{-2t})(1-x+xe^t) dt = \\ &= \frac{(1-x)^2}{4} (2 - e^{-2} + e^{-4}) + x(1-x)(1 - e^{-1} + e^{-2}). \end{aligned}$$

Функция $m(x)$ достигает максимального значения при $x \approx 0,382$,

$$m(0,382) \approx 0,397, \quad M\ell(\omega; 0,382) \approx 0,438, \quad m_\theta = 1,5, \quad K = 1,$$

поэтому из (4) получаем оценку средней временной выгоды

$$0,265 \leq H_*(\theta, \ell, x_0) \leq 0,292,$$

которая справедлива для почти всех $\sigma \in \Sigma$.

Список литературы / References

- [1] Ризниченко Г.Ю., *Лекции по математическим моделям в биологии. Ч. 1*, НИЦ "Регулярная и хаотическая динамика", Ижевск, 2002; [Riznichenko G.Yu., *Lektsii po matematicheskim modelyam v biologii. Ch. 1*, NIC "Regulyarnaya i haoticheskaya dinamika", Izhevsk, 2002, (in Russian).]
- [2] Bainov D.D., "Population dynamics control in regard to minimizing the time necessary for the regeneration of a biomass taken away from the population", *Applied Mathematics and Computation*, **39:3** (1990), 37–48.
- [3] Belyakov A.O., Davydov A.A., Veliov V.M., "Optimal cyclic exploitation of renewable resources", *J. Dyn. Control Syst.*, **21:3** (2015), 475–494.
- [4] Беляков А.О., Давыдов А.А., "Оптимизация эффективности циклического использования возобновляемого ресурса", *Тр. Ин-та матем. и механ. УрО РАН*, **22:2** (2016), 38–46; [Belyakov A.O., Davydov A.A., "Efficiency optimization for the cyclic use of a renewable resource", *Trudy Inst. Mat. i Mekh. UrO RAN*, **22:2** (2016), 38–46, (in Russian).]
- [5] Aseev S., Manzoor T., *Optimal growth, renewable resources and sustainability*, International Institute for Applied Systems Analysis (IIASA), Laxenburg, Austria, 2016.
- [6] Reed W.J., "Optimal escapement levels in stochastic and deterministic harvesting models", *Journal of Environmental Economics and Management*, **6** (1979), 350–363.
- [7] Капаун У., Quaas M. F., "Does the optimal size of a fish stock increase with environmental uncertainties?", *Economics Working Paper*, 2012, № 2012-09, 1–40.
- [8] Clark C., Kirkwood G., "On uncertain renewable resource stocks: Optimal harvest policies and the value of stock surveys", *Journal of Environmental Economics and Management*, **13:3** (1986), 235–244.
- [9] Reed W.J., Clarke H.R., "Harvest decisions and asset valuation for biological resources exhibiting size-dependent stochastic growth", *International Economic Review*, **31** (1990), 147–169.
- [10] Weitzman M.L., "Landing fees vs harvest quotas with uncertain fish stocks", *Journal of Environmental Economics and Management*, **43** (2002), 325–338.
- [11] Родина Л.И., "Оптимизация средней временной выгоды для вероятностной модели популяции, подверженной промыслу", *Вестн. Удмуртск. ун-та. Матем. Мех. Компьют. науки*, **28:1** (2018), 48–58; [Rodina L.I., "Optimization of average time profit for a probability model of the population subject to a craft", *Vestn. Udmurtsk. Univ. Mat. Mekh. Komp. Nauki*, **28:1** (2018), 48–58, (in Russian).]
- [12] Родина Л.И., Хаммади А.Х., "Статистические характеристики множества достижимости управляемых систем со случайными коэффициентами", *Известия вузов. Математика*, 2014, № 11, 50–63; English transl.: Rodina L.I., Khammadi A.K., "Statistical characteristics of attainability set of controllable systems with random coefficients", *Russian Mathematics (Iz. VUZ)*, **58:11** (2014), 43–53.
- [13] Родина Л.И., Тютеев И.И., "Об асимптотических свойствах решений разностных уравнений со случайными параметрами", *Вестн. Удмуртск. ун-та. Матем. Мех. Компьют. науки*, **26:1** (2016), 79–86; [Rodina L.I., Tyuteev I.I., "About asymptotical properties of solutions of difference equations with random parameters", *Vestn. Udmurtsk. Univ. Mat. Mekh. Komp. Nauki*, **26:1** (2016), 79–86, (in Russian).]

- [14] Ширяев А. Н., *Вероятность*, Наука, М., 1989; [Shiryaev A. N., *Veroyatnost*, Nauka, Moscow, 1989, (in Russian).]
- [15] Феллер В., *Введение в теорию вероятностей и ее приложения*. Т. 2, Мир, М., 1984; [Feller V., *Vvedenie v teoriyu veroyatnostej i ee prilozheniya*. V. 2, Mir, Moscow, 1984, (in Russian).]
- [16] Филиппов А. Ф., *Введение в теорию дифференциальных уравнений*, Едиториал УРСС, М., 2004; [Filippov A. F., *Vvedenie v teoriyu differencial'nyh uravnenij*, Editorial URSS, Moscow, 2004, (in Russian).]
- [17] Чаплыгин С. А., *Новый метод приближенного интегрирования дифференциальных уравнений*, Гостехиздат, М.–Л., 1950; [Chaplygin S. A., *Novyj metod priblizhennogo integrirvaniya differencialnyh uravnenij*, Gostekhizdat, M.–L., 1950, (in Russian).]

Rodina L. I., Tyuteev I. I., "On Estimation of an Average Time Profit in Probabilistic Environmental and Economic Models", *Modeling and Analysis of Information Systems*, **25:3** (2018), 257–267.

DOI: 10.18255/1818-1015-2018-3-257-267

Abstract. We consider environmental-economical models of optimal harvesting, given by the differential equations with impulse action, which depend on random parameters. We assume, that lengths of intervals θ_k between the moments of impulses τ_k are random variables and the sizes of impulse influence depend on random parameters v_k , $k = 1, 2, \dots$. One example of such objects is an equation with impulses, modelling dynamics of the population subject to harvesting. In the absence of harvesting, the population development is described by the differential equation $\dot{x} = g(x)$ and in time moments τ_k some random share of resource v_k , $k = 1, 2, \dots$ is taken from population. We can control gathering process so that to stop harvesting when its share will appear big enough to keep possible biggest the rest of a resource to increase the size of the following gathering. Let the equation $\dot{x} = g(x)$ have an asymptotic stable solution $\varphi(t) \equiv K$ and the interval (K_1, K_2) is the attraction area of the given solution (here $0 \leq K_1 < K < K_2$). We construct the control $u = (u_1, \dots, u_k, \dots)$, limiting a share of harvesting resource at each moment of time τ_k , so that the quantity of the remained resource, since some moment τ_{k_0} , would be not less than the given value $x \in (K_1, K)$. For any $x \in (K_1, K)$ the estimations of average time profit, valid with probability one, are received. It is shown, that there is a unique $x^* \in (K_1, K)$, at which the lower estimation reaches the greatest value. Thus, we described the way of population control at which the value of average time profit can be lower estimated with probability 1 by the greatest number whenever possible.

Keywords: model of a population subject to harvesting, average time profit, optimal exploitation

On the authors:

Lyudmila I. Rodina, orcid.org/0002-0007-1896-0951, Doctor of Physics and Mathematics, Professor of the Department of Functional Analysis and its Applications, Vladimir State University named after Alexander and Nikolay Stoletovs, 87 Gorky str., Vladimir, 600000 Russia, e-mail: LRodina67@mail.ru

Ilya I. Tyuteev, orcid.org/0009-0203-2514-7755, graduate student, Udmurt State University, 1 Universitetskaya str., Izhevsk, 426034, Russia, e-mail: it.30@mail.ru

Acknowledgments:

This work was supported by Russian Foundation of Basic Researches, project No 16-01-00346-a.

Динамические системы

©Кириллов А. Н., Данилова И. В., 2017

DOI: 10.18255/1818-1015-2018-3-268-275

УДК 517.977

Динамика распределения популяции по ареалам

Кириллов А. Н., Данилова И. В.

получена 30 декабря 2017

Аннотация. Рассматривается задача выбора популяцией ареала в условиях отсутствия у неё полной информации о полезности ареала, то есть об объеме у него энергетических ресурсов. Данная задача относится к теории оптимального фуражирования. У. Дикман (U. Dieckmann) предложил подход к моделированию распределения популяции по ареалам, основанный на функции полезности, учитывающей количество ресурсов в ареале, расстояние от популяции до него и меру информированности популяции о количестве ресурсов в ареале. При этом используется распределение Больцмана для описания распределения популяции по ареалам. Рассматривается статическая задача, не учитывающая изменение положения популяции с течением времени. В настоящей работе предложена динамическая система, описывающая распределение популяции по ареалам, зависящее от полезности ареалов, которая изменяется со временем вследствие изменения расстояния от популяции до ареала. При этом распределение Больцмана является частным решением полученной системы обыкновенных дифференциальных уравнений. Получено условие устойчивости по Ляпунову распределения Больцмана. Введены функции полезности ареалов, зависящие от расстояния до ареала и меры информированности популяции об ареале. В результате, в двумерном случае, пространство R^2 разбивается на области предпочтительной полезности. Такое разбиение является обобщением диаграммы Г.Ф. Вороного.

Ключевые слова: динамика популяции, ареал, функция полезности, устойчивость, распределение Больцмана

Для цитирования: Кириллов А. Н., Данилова И. В., "Динамика распределения популяции по ареалам", *Моделирование и анализ информационных систем*, 25:3 (2018), 268–275.

Об авторах:

Кириллов Александр Николаевич, orcid.org/0000-0002-3356-1846, д-р физ.-мат. наук, Институт прикладных математических исследований Карельского научного центра РАН, Пушкинская ул., 11, г. Петрозаводск, 185910 Россия, Петрозаводский государственный университет, просп. Ленина, 33, г. Петрозаводск, 185910 Россия, e-mail: kirillov@krc.karelia.ru

Данилова Инна Владимировна, orcid.org/0000-0001-7031-4580, аспирант, Институт прикладных математических исследований Карельского научного центра РАН, Пушкинская ул., 11, г. Петрозаводск, 185910 Россия, e-mail: DanilovaInna1987@mail.ru

Благодарности:

Работа выполнена при поддержке РФФИ, грант 18-01-00249а.

Введение

Теория оптимального фуражирования предполагает, что популяция в поисках пищи действует таким образом, чтобы максимизировать скорость потребления энергии.

Основные задачи теории фуражирования: нахождение условий ухода популяции из ареала, выбор наиболее пригодного ареала, моделирование перемещения популяции между ареалами. Основным результатом в решении задачи об уходе из ареала является теорема о маргинальных значениях: популяция покидает ареал, когда мгновенная скорость потребления энергии в нем снизится до средней скорости потребления энергии [1]. Для моделирования движения популяции предложено большое разнообразие моделей, основанных на случайных процессах [2], [3], [4]. Для решения задачи выбора ареала S. D. Fretwell и H. L. Lukas разработали теорию идеального свободного распределения (Ideal free distribution, IFD) [5], для предсказания выбора популяцией среды обитания. Идеальное свободное распределение – теоретико-игровая концепция, которая предполагает, что популяция перемещается между ареалами мгновенно и имеет точную информацию о качестве ареалов.

Распределение популяции по m ареалам называется идеальным свободным распределением, если выполняются два условия: популяция занимает $k < m$ ареалов и в занятых популяцией k ареалах скорость потребления энергии максимальна и одинакова, а в незанятых достаточно мала. Эмпирические исследования показали расхождение модели идеального свободного распределения с реальностью: ареалы худшего качества также привлекают особей популяции, отсутствие равной конкуренции и точного знания о качестве ареалов, передвижение между ареалами требует затрат.

В настоящей работе предлагается подход к решению задачи выбора популяцией ареала. При этом описывается динамика поведения популяции при выборе ареала без описания движения детерминированными или стохастическими моделями. Это связано с тем, что модель движения популяции зависит от вида популяции и условий движения, и поэтому общий подход к моделированию движения, по мнению авторов, невозможен. Предлагаемая модель описывает динамику вероятностей выбора популяцией того или иного ареала. Используется подход, предложенный У. Дикманом (U. Dieckmann) [6], где введена функция полезности, учитывающая количество ресурсов в ареале, расстояние от популяции до него и меру информированности популяции о количестве ресурсов в ареале. В отличие от концепции IFD, недостатки которой анализируются в [6], У. Дикман использует распределение Больцмана для описания распределения популяции по ареалам. При этом рассматривается статическая задача, не учитывающая изменение положения популяции с течением времени.

В настоящей работе предложена динамическая система, описывающая распределение популяции по ареалам, зависящее от полезности ареалов, которая изменяется со временем вследствие изменения расстояния от популяции до ареала. При этом распределение Больцмана является частным решением полученной системы обыкновенных дифференциальных уравнений. Получено условие устойчивости по Ляпунову распределения Больцмана. Введены функции полезности ареалов, зависящие от расстояния до ареала и меры информированности популяции об ареале. В результате, в двумерном случае, пространство R^2 разбивается на области предпочтительной полезности. Такое разбиение является обобщением диаграммы Г.Ф. Вороного.

1. Области предпочтительной полезности

В настоящей работе рассматривается некоторое пространство, содержащее ареалы, т.е. области, в которых содержатся запасы энергии (питательные ресурсы), необходимые популяции. При этом популяция некоторым образом перемещается в данном пространстве и в каждый момент времени t оценивает полезность ареалов с целью выбора наиболее подходящего для неё. Полезность ареала с точки зрения популяции определяется расстоянием до него, мерой информированности о его истинной полезности в данный момент времени и затратами на перемещение к нему.

Пусть $P_i = P_i(t)$ — вероятность выбора популяцией ареала с номером i , $i = 1, \dots, m$, в момент времени t . Поставим задачу описания динамики изменения вероятностей $P_i(t)$, т.е. задачу построения математической модели динамики распределения популяции по ареалам. При этом будем предполагать, что вероятность $P_i(t)$ зависит от функции полезности $U_i = U_i(d_i)$ ареала i с точки зрения популяции, находящейся от него на расстоянии $d_i = d_i(t)$. В разделе 2 будет предложена динамическая система, описывающая изменение $P_i(t)$, $i = 1, \dots, m$. При этом в основе этой динамической системы лежит распределение Больцмана, которое также использовано в работе [6]. В разделе 3 доказана устойчивость по Ляпунову распределения Больцмана, являющегося частным решением соответствующей системы обыкновенных дифференциальных уравнений.

В настоящем разделе вводится понятие *области предпочтительной полезности* (ОПП) ареала. Смысл этого понятия состоит в том, что, находясь в области предпочтительной полезности, популяция с большей вероятностью выберет ареал, находящийся в этой области.

Введем следующие обозначения. Пусть m — количество ареалов, под ареалом будем понимать фиксированную точку A_i из пространства R^n и при этом каждый ареал имеет запас энергии V_i , $i = 1, \dots, m$. Точка $M(t) = M \in R^n$ характеризует положение популяции в пространстве в момент времени t , $d_i(t) = \rho(M(t), A_i)$ — расстояние от популяции до i -го ареала в момент времени t . В работе [6] введена функция полезности U_{ij} для задачи выбора популяцией j -го ареала при условии, что она находится в i -м ареале и неподвижна. В настоящей работе популяция движется, оценивая в каждый момент времени полезность U_i ареалов A_i . Используя подход к понятию полезности из [6], введем функцию полезности $U_i(d_i)$ ареала A_i для популяции, находящейся на расстоянии $d_i = d_i(t)$ от него:

$$U_i(d_i) = I(d_i)V_i - T(d_i) + (1 - I(d_i))\bar{V}, i = 1, \dots, m, \quad (1)$$

где $U_i(d_i)$ — полезность i -го ареала с точки зрения популяции, находящейся на расстоянии d_i от него; $I(d_i)$ — мера информированности популяции, находящейся на расстоянии d_i от ареала A_i , $I(d_i) \in (0, 1]$; $T(d_i)$ — затраты на перемещение к ареалу A_i ; $\bar{V} = \sum_{i=1}^m I(d_i)V_i$ — средняя информированность популяции об ареалах.

Определим понятие области предпочтительной полезности (ОПП).

Определение. Область предпочтительной полезности D_i ареала A_i — это множество точек M вида

$$D_i = \{M \in R^n : U_i(\rho(M, A_i)) > U_j(\rho(M, A_j)), i \neq j, j = 1, \dots, m\}.$$

Замечание. Если в формуле (1) отбросить первое и третье слагаемые, т.е. не учитывать информированность, а в качестве функции затрат $T_i(d_i)$ взять d_i , то разбиение пространства с ареалами на ОПП в случае $n = 2$ при $U_i(d_i) = -d_i$ является диаграммой Вороного.

1.1. Двумерный случай

Рассмотрим пример построения области предпочтительной полезности в случае двух ареалов, находящихся в пространстве R^2 .

Пусть $M \in R^2$, $M = (x, y)$, $A_1 = (-1, 0)$, $A_2 = (1, 0)$, то есть ареалы — точки из R^2 . Расстояния от популяции $M = (x, y)$ до ареалов равны: $d_1 = \sqrt{(x+1)^2 + y^2}$ и $d_2 = \sqrt{(x-1)^2 + y^2}$. Введем функции полезности ареалов, с учетом расстояния до каждого из них и меры информированности:

$$U_i(d_i) = e^{-\beta d_i^2} V_i - \alpha d_i^2. \quad (2)$$

$I(d_i) = e^{-\beta d_i^2}$ — мера информированности об i -м ареале у популяции, находящейся на расстоянии d_i от i -го ареала, β — коэффициент "забывания" информации об ареале. Чем меньше β , тем медленнее "забывается" информация об истинной полезности V_i ареала при удалении популяции от него (см. рис. 1), $T(d_i) = \alpha d_i^2$ — затраты популяции при перемещении к i -му ареалу на расстояние d_i . Пусть $V_2 > V_1$. Заметим, что мера информированности об i -м ареале, $I(d_i)$, максимальна при $d_i = 0$ и $I(d_i) \rightarrow 0$ при $d_i \rightarrow \infty$.

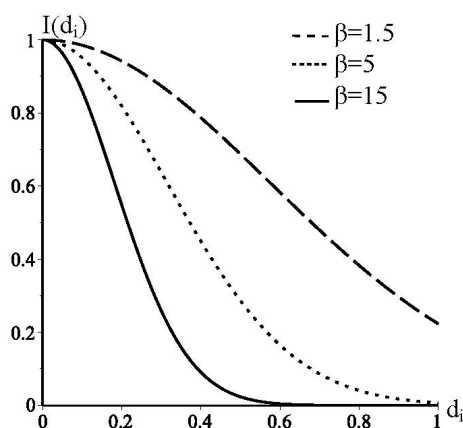
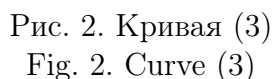


Рис. 1. Мера информированности
Fig. 1. Measure of information

Области предпочтительных полезностей имеют вид: $D_1 = \{(x, y) : U_1(d_1) > U_2(d_2)\}$, $D_2 = \{(x, y) : U_2(d_2) > U_1(d_1)\}$. Найдем общую границу областей D_1 и D_2 , приравняв $e^{-\beta d_1^2} V_1 - \alpha d_1^2 = e^{-\beta d_2^2} V_2 - \alpha d_2^2$. Учитывая выражение для d_1 и d_2 , после несложных преобразований получаем

$$y^2 = \frac{1}{\beta} \ln \frac{V_1 e^{-2\beta x} - V_2 e^{2\beta x}}{4\alpha e^{\beta(x^2+1)x}}. \quad (3)$$

График кривой (3), являющейся общей границей областей D_1 и D_2 , изображен на рис. 2.



где $\varphi_{ij}(t) = \dot{U}_i - \dot{U}_j$.

Рассмотрим случай двух ареалов, $m = 2$:

$$\begin{cases} \dot{P}_1 = q \cdot P_1 \cdot P_2 \cdot \varphi(t) \\ \dot{P}_2 = -q \cdot P_1 \cdot P_2 \cdot \varphi(t), \end{cases} \quad (4)$$

где $\varphi_{12}(t) = \varphi(t)$.

Найдем решения $P_1(t)$ и $P_2(t)$ системы дифференциальных уравнений (4). Учитывая, что $P_1 + P_2 = 1$, получим $\dot{P}_1 = q \cdot P_1 \cdot (1 - P_1) \cdot \varphi(t)$. Интегрируя это уравнение, получим

$$P_1(t) = \frac{P_{10}e^{q\Phi(t)}}{1 + P_{10}(e^{q\Phi(t)} - 1)}, P_2(t) = \frac{1 - P_{10}}{1 + P_{10}(e^{q\Phi(t)} - 1)} \quad (5)$$

где $\Phi(t) = U_1(t) - U_2(t) - U_1(0) + U_2(0)$, $P_{10} = P_1(0)$ и $P_{20} = P_2(0)$. Несложно показать, что решение (5) совпадает с распределением Больцмана

$$\tilde{P}_1(t) = \frac{e^{qU_1(t)}}{e^{qU_1(t)} + e^{qU_2(t)}}, \tilde{P}_2(t) = \frac{e^{qU_2(t)}}{e^{qU_1(t)} + e^{qU_2(t)}}$$

при $P_{10}e^{-U_1(0)} = P_{20}e^{-U_2(0)}$.

3. Устойчивость распределения Больцмана

Исследуем устойчивость распределения Больцмана в случае двух ареалов ($m = 2$).

Теорема 1. Пусть $\varphi(t)$ непрерывна, тогда решение системы (4), являющееся распределением Больцмана, устойчиво по Ляпунову.

Доказательство. Введем для удобства обозначения $\tilde{P}_1(t) = \tilde{P}(t)$, $P_1(t) = P(t)$, $\tilde{P}_1(0) = \tilde{P}_0$, $P_1(0) = P_0$, $U_{20} = U_2(0)$ и $U_{10} = U_1(0)$. После несложных преобразований получим $\tilde{P}(t) = \frac{1}{1 + e^{q(U_2(t) - U_1(t))}}$ и $P(t) = \frac{P_0}{P_0 + (1 - P_0)e^{-q\Phi(t)}}$. Пусть $g(t) = e^{q(U_2(t) - U_1(t))}$, $g(0) = e^{q(U_{20} - U_{10})}$ и $P_0 - \tilde{P}_0 = P_0 - \frac{1}{1 + g(0)} = \alpha$. Тогда $|P(t) - \tilde{P}(t)| = \left| \frac{g(t)}{(1 + (\frac{1}{P_0} - 1)\frac{g(t)}{g(0)})(1 + g(t))} (1 - \frac{\frac{1}{P_0} - 1}{g(0)}) \right|$, где $1 - \frac{\frac{1}{P_0} - 1}{g(0)} = \frac{\alpha(1 + g(0))^2}{g(0)(1 + \alpha + \alpha g(0))} = h(\alpha)$. Пусть $\beta = \alpha(1 + g(0))$, тогда $h(\alpha) = \frac{\beta(1 + g(0))}{g(0)(1 + \beta)}$. Отсюда следует $|P(t) - \tilde{P}(t)| = \left| \frac{g(t)}{(1 + (\frac{1}{P_0} - 1)\frac{g(t)}{g(0)})(1 + g(t))} (1 - \frac{\frac{1}{P_0} - 1}{g(0)}) \right| < C \left| \frac{\beta(1 + g(0))}{g(0)(1 + \beta)} \right| < \varepsilon$, где $C = \text{const}$ и $C > 0$, очевидно, что $\left| \frac{g(t)}{(1 + (\frac{1}{P_0} - 1)\frac{g(t)}{g(0)})(1 + g(t))} \right| < C$ при любом поведении $g(t)$. Отсюда следует, что $-A < \frac{\beta}{(1 + \beta)} < A$, где $A = \frac{\varepsilon}{C(\frac{1 + g(0)}{g(0)})}$. Пусть ε достаточно мало, что согласуется с определением устойчивости, тогда $0 < A < 1$ и $-\frac{A}{1 + A} < \beta < \frac{A}{1 - A}$. Отсюда следует, что $-\frac{\varepsilon g(0)}{C + \frac{\varepsilon g(0)}{1 + g(0)}} < \alpha < \frac{\varepsilon g(0)}{C - \frac{\varepsilon g(0)}{1 + g(0)}}$. Пусть $B_1 = \frac{\varepsilon g(0)}{C + \frac{\varepsilon g(0)}{1 + g(0)}}$, $B_2 = \frac{\varepsilon g(0)}{C - \frac{\varepsilon g(0)}{1 + g(0)}}$, и $B = \min(B_1, B_2)$. Тогда если $-B < \alpha < B$, то $|P_0 - \tilde{P}_0| = |\alpha| < B$, то есть достаточно взять $\delta = B$. Отсюда следует устойчивость по Ляпунову. Теорема доказана. $\square$

Вид решения системы (4) зависит от вида функции $\varphi(t)$. На рисунках 3 и 4 показаны решения системы (4) при $\varphi(t) = \cos(t)$ и $\varphi(t) = t^2 e^{-t^2}$. На рисунке 3 показано, что решения системы (4) являются периодическими, если $\varphi(t)$ — ограниченная периодическая функция. На рисунке 4 показано, что решения системы (4) не являются периодическими, если $\varphi(t)$ — ограниченная функция.

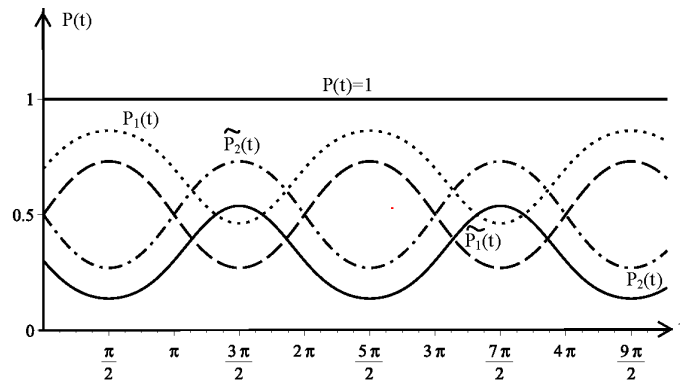

 Рис. 3. Периодическое решение при $\varphi(t) = \cos(t)$, $P_{10} = 0,7$

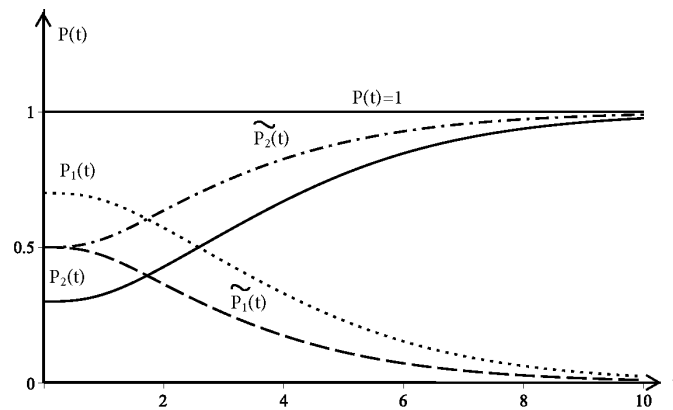
 Fig. 3. Periodical solution with $\varphi(t) = \cos(t)$, $P_{10} = 0,7$

 Рис. 4. Непериодическое решение при $\varphi(t) = t^2 e^{-t^2}$, $P_{10} = 0,7$

 Fig. 4. Not periodical solution with $\varphi(t) = t^2 e^{-t^2}$, $P_{10} = 0,7$

4. Заключение

В работе была построена функция полезности в задаче выбора одного из двух ареалов, с учетом расстояния до каждого из них, меры информированности об ареале и затрат на перемещение к нему. Была предложена система дифференциальных уравнений, описывающих динамику вероятности выбора ареала и проведен анализ устойчивости распределения Больцмана.

Список литературы / References

- [1] Charnov E. L., "Optimal foraging, the marginal value theorem", *Theoretical Population Biology*, **9** (1976), 129–136.
- [2] Patlak C. S., "Random walk with persistence and external bias", *Bulletin of Mathematical Biophysics*, **15** (1953), 311–338.
- [3] Hoffmann G., "Optimization of Brownian search strategies", *Biological Cybernetics*, **49** (1983), 21–31.
- [4] Bovet P., Benhamou S., "Spatial analysis of animals' movements using a correlated random walk model", *Journal of Theoretical Biology*, **131**:4 (1988), 419–433.

- [5] Fretwell S. D., Lucas H. L., "On territorial behavior and other factors influencing habitat distribution in birds", *Acta Biotheoretica*, **19** (1970), 16–36.
- [6] Shuichi M., Arlinghaus R., Dieckmann U., "Foraging on spatially distributed resources with sub-optimal movement, imperfect information, and travelling costs: departures from the ideal free distribution", *Synthesizing Ecology*, **119:9** (2010), 1469–1483.

Kirillov A. N., Danilova I. V., "Dynamics of Population Patch Distribution", *Modeling and Analysis of Information Systems*, **25:3** (2018), 268–275.

DOI: 10.18255/1818-1015-2018-3-268-275

Abstract. The problem of selection by the patch population in the absence of information on the utility of the patch, that is, the volume of its energy resources, is considered. This problem relates to the theory of optimal foraging. U. Dieckman proposed an approach to modeling the population patch distribution. The approach is based on a utility function that takes into account the amount of resources in a patch, the population – patch distance, and the measure of information certainty on patch utility. In this case, the Boltzmann distribution is used to describe the population patch distribution. And U. Dieckman considered a static problem that does not take into account the change in the position of the population with time. In this paper, we propose a dynamic system that describes the population patch distribution, which depends on the utility of the patch. In addition the utility varies with time as a result of distance variations. The Boltzmann distribution is a particular solution of the proposed system of differential equations. The Lyapunov stability condition for the Boltzmann distribution is obtained. The utility functions of the patches, which depend on the population – patch distance and on the measure of the information certainty, are introduced. As a result, in the two-dimensional case, a space R^2 is divided into areas of preferred utility. Such a partition is a generalization of the Voronoi diagram.

Keywords: population dynamics, the patch, utility function, stability, Boltzmann distribution

On the authors:

Alexander N. Kirillov, orcid.org/0000-0002-3356-1846, Doctor of Science,
Institute of Applied Mathematical Research of the Karelian Research Centre RAS,
11 Pushkinskaya Str., 185910 Petrozavodsk, Russia,
Petrozavodsk State University,
33 Lenina prosp., 185910 Petrozavodsk, Russia, e-mail: kirillov@krc.karelia.ru

Inna V. Danilova, orcid.org/0000-0001-7031-4580, graduate student,
Institute of Applied Mathematical Research of the Karelian Research Centre RAS,
11 Pushkinskaya Str., 185910 Petrozavodsk, Russia, e-mail: DanilovaInna1987@mail.ru

Acknowledgments:

This paper was supported by the RFBR (18-01-00249a).

Криптосистемы

©Косолапов Ю. В., Шигаев А. Н., 2018

DOI: 10.18255/1818-1015-2018-3-276-290

УДК 517.9

Об алгоритме расщепления носителя для индуцированных кодов

Косолапов Ю. В., Шигаев А. Н.

получена 12 февраля 2018

Аннотация. В 2000 г. Н. Сендриер показал, что если для линейного $[n, k, d]$ -кода $C(\subseteq \mathbb{F}_q^n)$ длины n и размерности k с кодовым расстоянием d группа автоморфизмов $\text{RAut}(C)$ этого кода тривиальна, то может быть построен детерминированный алгоритм расщепления носителя, позволяющий для кода D , перестановочно-эквивалентного коду C , найти такую перестановку σ , что $\sigma(C) = D$. Этот алгоритм, в частности, может быть применен для осуществления атаки на ключ кодовой криптосистемы типа Мак-Элиса на коде C . Целью настоящей работы является построение и анализ алгоритма расщепления носителя для кода $\mathbb{F}_q^l \otimes C$, индуцированного кодом C , $l \in \mathbb{N}$. Так как группа автоморфизмов $\text{RAut}(\mathbb{F}_q^l \otimes C)$ нетривиальна даже в случае, когда группа автоморфизмов базового кода C тривиальна, то это позволяет предположить потенциально высокую стойкость криптосистемы типа Мак-Элиса на коде $\mathbb{F}_q^l \otimes C$ к атаке на основе расщепления носителя. В работе строится алгоритм расщепления носителя для кода $\mathbb{F}_q^l \otimes C$ и сравнивается эффективность этого алгоритма с имеющейся атакой на ключ криптосистемы типа Мак-Элиса на основе кода $\mathbb{F}_q^l \otimes C$.

Ключевые слова: групповые коды, индуцированные групповые коды, алгоритм расщепления носителя, криптосистема Мак-Элиса

Для цитирования: Косолапов Ю. В., Шигаев А. Н., "Об алгоритме расщепления носителя для индуцированных кодов", *Моделирование и анализ информационных систем*, 25:3 (2018), 276–290.

Об авторах:

Косолапов Юрий Владимирович, orcid.org/0000-0002-1491-524X, канд. техн. наук,
Южный Федеральный Университет,
ул. Большая Садовая, 105/42, г. Ростов-на-Дону, 344006, Россия, e-mail: itaim@mail.ru,

Шигаев Алексей Николаевич, orcid.org/0000-0001-6363-4332, магистр,
Южный Федеральный Университет,
ул. Большая Садовая, 105/42, г. Ростов-на-Дону, 344006, Россия, e-mail: aleksejshig@gmail.com

1. Введение

В постквантовую эпоху кодовые криптосистемы типа Мак-Элиса [1] рассматриваются как возможные альтернативы тем асимметричным криптосистемам, стойкость которых в настоящее время основана на сложности факторизации больших целых чисел или на сложности дискретного логарифмирования в конечной группе [2]. Необходимым условием построения криптосистем типа Мак-Элиса на основе

линейных кодов является существование для этих кодов эффективных (полиномиальных) алгоритмов декодирования. Однако это условие не является достаточным. В частности, например, для кодов Рида–Соломона и кодов Рида–Маллера имеются быстрые алгоритмы декодирования [3], однако, как показано в [4] и [5], соответствующие криптосистемы типа Мак–Элиса на этих кодах не являются стойкими к атакам на ключ (к структурным атакам). Результаты исследования стойкости криптосистем типа Мак–Элиса показывают, что чем более код похож по структуре на случайный код, тем сложнее анализ соответствующей криптосистемы типа Мак–Элиса. Одним из возможных способов построения стойкой криптосистемы типа Мак–Элиса является поиск или построение кода, для которого, с одной стороны, имеется эффективный декодер, а с другой стороны, который похож на случайный.

В [6] показано, что если для базового кода C существует эффективный мажоритарный декодер, то для индуцированного кода $\mathbb{F}_q^l \otimes C$, $l \in \mathbb{N}$, также может быть построен эффективный мажоритарный декодер. В связи с этим в [7] предложена криптосистема типа Мак–Элиса на основе индуцированного кода $\mathbb{F}_q^l \otimes C$. При этом установлено, что если криптосистема типа Мак–Элиса на основе базового кода C является нестойкой к атакам на ключ, то атакующий хотя и может построить атаку на ключ для соответствующей криптосистемы на основе индуцированного кода $\mathbb{F}_q^l \otimes C$, однако эта атака не будет эффективной при тщательном подборе параметров индуцированного кода.

Целью настоящей работы является построение алгоритма расщепления носителя для индуцированных кодов и оценка эффективности его применения при нахождении секретного ключа кодовой криптосистемы типа Мак–Элиса на основе индуцированного кода $\mathbb{F}_q^l \otimes C$. Работа имеет следующую структуру. Вторым разделом содержит необходимые сведения о кодах, об алгоритме расщепления носителя и предварительные результаты об индуцированных кодах. Также здесь строится алгоритм расщепления носителя для индуцированных кодов. В третьем разделе рассматривается применение этого алгоритма для нахождения секретной перестановки криптосистемы типа Мак–Элиса на индуцированном коде, сравнивается эффективность построенного алгоритма с эффективностью алгоритма из работы [7]. Дополнительно рассматривается возможное применение индуцированных кодов в алгоритме идентификации.

2. Алгоритм расщепления носителя для индуцированных кодов

2.1. Предварительные сведения

Пусть $\mathbb{F}_q$ — поле Галуа мощности q , где q — степень простого числа. Для вектора $\mathbf{x}$ из пространства $\mathbb{F}_q^n$ размерности n определим вес $\text{wt}(\mathbf{x})$ как мощность множества ненулевых координат вектора $\mathbf{x}$. В пространстве $\mathbb{F}_q^n$ рассмотрим $[n, k, d]$ -код C размерности k , длины n с кодовым расстоянием d . Пусть $G(C)$ — порождающая матрица кода, $C \subseteq \mathbb{F}_q^n$. Коды C и D размерности k и длины n называются перестановочно-эквивалентными, если существует такая перестановка σ из группы симметрической

группы S_n , действующей на элементах множества $I_n = \{1, \dots, n\}$, что

$$D = \{(c_1, \dots, c_n) | (c_{\sigma^{-1}(1)}, \dots, c_{\sigma^{-1}(n)}) \in C\}.$$

В этом случае будет использоваться принятое обозначение $D = \sigma(C)$. Далее нам понадобятся определения инварианта и сигнатуры из [8]. Для некоторого подмножества $J(\subseteq I_n)$ символом C_J обозначим множество векторов, полученных из векторов кода C путем зануления координат с номерами из J . Пусть $\mathcal{L}_n$ – множество всех кодов длины n , $\mathcal{L} = \bigcup_{n>0} \mathcal{L}_n$. Отображение $\mathcal{V} : \mathcal{L} \rightarrow E$ называется *инвариантом* над множеством E , если для любых двух перестановочно-эквивалентных кодов C и D выполняется равенство: $\mathcal{V}(C) = \mathcal{V}(D)$. *Сигнатурой* над множеством F называется отображение $\mathcal{S} : \mathcal{L}_n \times I_n \rightarrow F$, такое, что для любой перестановки $\sigma(\in S_n)$ и любого кода $C \in \mathcal{L}_n$ выполняется равенство: $\mathcal{S}(C, i) = \mathcal{S}(\sigma(C), \sigma(i))$. Далее мы будем рассматривать только сигнатуры, которые построены на основе инварианта по следующему правилу:

$$\mathcal{S}(C, i) = \mathcal{V}(C_i), \quad (1)$$

где $C_i = C_{\{i\}}$. Дискриминантом кода C называется такая сигнатура $\mathcal{S}$, для которой существуют такие i и j из I_n , что $\mathcal{S}(C, i) \neq \mathcal{S}(C, j)$. Тогда *полным дискриминантом* для кода C называется такая сигнатура $\mathcal{S}$, что $\mathcal{S}(C, i) \neq \mathcal{S}(C, j)$ для всех разных i и j из I_n . Приведем в виде леммы известный факт.

Лемма 1. Пусть C – $[n, k, d]$ -код, $\sigma \in S_n$, $D = \sigma(C)$. Равенство $D = \gamma(C)$ выполняется тогда и только тогда, когда $\gamma \in \sigma \text{PAut}(C)$, где $\sigma \text{PAut}(C)$ – фактор-класс из фактор-множества $S_n / \text{PAut}(C)$.

Доказательство. Очевидно, что если $\gamma \in \sigma \text{PAut}(C)$, то $D = \gamma(C)$. Докажем в обратную сторону. Предположим, что выполняется равенство $D = \gamma(C)$, но $\gamma \notin \sigma \text{PAut}(C)$. Так как $\gamma(C) = \sigma(C)$, то $\gamma^{-1}\sigma \in \text{PAut}(C)$. Отсюда получаем, что имеет место представление $\gamma^{-1} = \phi\sigma^{-1}$, $\phi \in \text{PAut}(C)$. Следовательно, $\gamma \in \sigma \text{PAut}(C)$. $\square$

Рассмотрим алгоритм SSA, который с помощью дискриминанта $\mathcal{S}$ находит такую перестановку σ' для двух перестановочно-эквивалентных кодов C и $D = \sigma(C)$, что $D = \sigma'(C)$. Заметим, что в общем случае $\sigma \neq \sigma'$, однако, в силу леммы 1, $\sigma'^{-1}\sigma \in \text{PAut}(C)$. Перестановку σ' , возвращаемую алгоритмом SSA, будем называть подходящей. Если $\mathcal{S}$ – полный дискриминант, то $\sigma = \sigma'$, при этом перестановка σ будет найдена на первой итерации цикла этого алгоритма. Как следует из утверждения 8 работы [8], для кода C полный дискриминант существует тогда и только тогда, когда группа автоморфизмов $\text{PAut}(C)$ кода C тривиальна. Отметим, что коды с тривиальной группой автоморфизмов существуют (см., например, [9]).

В [8] отмечено, что даже если существует полный дискриминант кода C , его вычисление может оказаться вычислительно сложным, поэтому в [8] предложена техника, которая может позволить построить вычислительно простые полные дискриминанты на основе неполных дискриминантов. Так как, в соответствии с (1), рассматриваются только сигнатуры, основанные на инвариантах, то необходимо, чтобы инварианты были также вычислительно простыми.

Исходные параметры: $C \in \mathcal{L}_n$, $D = \sigma(C)$, $\mathcal{S}$

Результат: $\sigma' : D = \sigma'(C)$

1. Вычислить $\mathcal{D} = (\mathcal{S}(D, i))_{i=1}^n$

2. Вычислить $\mathcal{C} = (\mathcal{S}(, i))_{i=1}^n$

3. $\Sigma = \emptyset$, $\text{exit} = \text{false}$;

до тех пор, пока $\text{exit}! = \text{true}$ **выполнять**

 Выбрать σ' из $S_n \setminus \Sigma$

если $\sigma'(C) \neq D$ **тогда**

 | $\Sigma = \Sigma \cup \{\sigma'\}$

конец условия

иначе

 | $\text{exit} = \text{true}$

конец условия

конец цикла

возвратить Ω

Алгоритм 1: SSA

Примером просто вычислимого инварианта для кодов малой размерности является отображение $\mathcal{V}^W : \mathcal{L} \rightarrow \mathbb{Z}[X]$, ставящее в соответствие коду C его нумератор весов $\mathcal{W}(C) = \sum_{i=0}^n W_i X^i$, где W_i — число векторов веса i в коде C , $\mathbb{Z}[X]$ — множество полиномов от одной переменной с коэффициентами из $\mathbb{Z}$. На основе этого инварианта может быть построена сигнатура $\mathcal{S}^W : \mathcal{L}_n \times I_n \rightarrow \mathbb{Z}[X]$, определенная по правилу: $\mathcal{S}^W(C, i) = \mathcal{V}^W(C_i) = \mathcal{W}(C_i)$. Заметим, что сложность вычисления инварианта $\mathcal{V}^W(C_i)$ растет неполиномиально с ростом размерности кода C_i . Поэтому в [8] дискриминант строится на основе вычисления нумератора весов остова кода. Под остовом (hull) кода C в [8] понимается пересечение кода C с его дуальным кодом $C^\perp$:

$$\mathcal{H}(C) = C \cap C^\perp. \quad (2)$$

Выбор этой характеристики кода обоснован тем, что размерность остова в среднем существенно меньше размерности кода C , что позволяет эффективно вычислять нумераторы и строить простые для вычисления дискриминанты даже в случае большой размерности кода C .

2.2. Индуцированные коды и их свойства

Пусть C^i — $[n_i, k_i, d_i]$ -код с порождающей матрицей $G(C^i)$ и проверочной матрицей $H(C^i)$, $i = 1, 2$. Под декартовым произведением $C^1 \times C^2$ кодов C^1 и C^2 будем понимать множество вида

$$C^1 \times C^2 = \{(\mathbf{a} \parallel \mathbf{b}) : \mathbf{a} \in C^1, \mathbf{b} \in C^2\},$$

где $\mathbf{a} \parallel \mathbf{b}$ — конкатенация векторов $\mathbf{a}$ и $\mathbf{b}$. Легко проверить, что порождающая и проверочная матрицы кода $C^1 \times C^2$ могут быть представлены в виде

$$G(C^1 \times C^2) = \begin{pmatrix} G(C^1) & O_{k_1 \times n_2} \\ O_{k_2 \times n_1} & G(C^2) \end{pmatrix}, \quad H(C^1 \times C^2) = \begin{pmatrix} H(C^1) & O_{n_1 - k_1 \times n_2} \\ O_{n_2 - k_2 \times n_1} & H(C^2) \end{pmatrix},$$

где $O_{a \times b}$ — нулевая $(a \times b)$ -матрица. Из определения (2) следует, что

$$\mathcal{H}(C^1 \times C^2) = \mathcal{H}(C^1) \times \mathcal{H}(C^2). \quad (3)$$

Лемма 2. Пусть C^i — $[n_i, k_i]$ -код, $\mathcal{W}(C^i) = \sum_{j=0}^{n_i} W_j^{(i)} X^{(i)}$ — нумератор кода C^i , $i = 1, 2$. Тогда нумератор кода $C^1 \times C^2$ имеет вид

$$\mathcal{W}(C^1 \times C^2) = \mathcal{W}(C^1) \cdot \mathcal{W}(C^2).$$

Доказательство. Каждый кодовый вектор $\mathbf{c}$ из $C^1 \times C^2$ представим в виде конкатенации $(\mathbf{a} \parallel \mathbf{b})$ двух векторов $\mathbf{a}$ и $\mathbf{b}$ из C^1 и C^2 соответственно. Найдем количество векторов веса j ($0 \leq j \leq n_1 + n_2$) в коде $C^1 \times C^2$. Для этого рассмотрим всевозможные упорядоченные пары (j_1, j_2) неотрицательных целых чисел таких, что $j_1 + j_2 = j$. Для каждой такой пары (j_1, j_2) в коде $C^1 \times C^2$ имеется множество из $W_{j_1}^{(1)} \cdot W_{j_2}^{(2)}$ векторов веса j . Для различных пар эти множества не пересекаются. Поэтому в коде $C^1 \times C^2$ будет всего

$$\sum_{(j_1, j_2): j_1 + j_2 = j} W_{j_1}^{(1)} \cdot W_{j_2}^{(2)}$$

векторов веса j . Отсюда следует

$$\mathcal{W}(C^1 \times C^2) = \sum_{j=0}^{n_1 + n_2} \left(\sum_{(j_1, j_2): j_1 + j_2 = j} W_{j_1}^{(1)} \cdot W_{j_2}^{(2)} \right) X^j = \mathcal{W}(C^1) \cdot \mathcal{W}(C^2).$$

□

Под тензорным произведением $A \otimes B$ матриц $A = (a_{i,j})_{i=1,m;j=1,l}$ и B будем понимать матрицу вида

$$A \otimes B = \begin{pmatrix} a_{1,1}B & \dots & a_{1,l}B \\ \dots & \dots & \dots \\ a_{m,1}B & \dots & a_{m,l}B \end{pmatrix}.$$

Пусть C — $[n, k, d]$ -код с порождающей матрицей $G(C)$, E_l — единичная матрица порядка l . Подпространство, порожденное строками матрицы $E_l \otimes G(C)$, обозначим $\mathbb{F}_q^l \otimes C$ и, в соответствии с [7], будем называть индуцированным кодом (кодом, который индуцирован кодом C). Порождающая матрица этого кода $G(\mathbb{F}_q^l \otimes C) = E_l \otimes G(C)$ имеет блочный вид

$$G(\mathbb{F}_q^l \otimes C) = \underbrace{\begin{pmatrix} G(C) & O_{k \times n} & \dots & O_{k \times n} \\ O_{k \times n} & G(C) & \dots & O_{k \times n} \\ \dots & \dots & \dots & \dots \\ O_{k \times n} & O_{k \times n} & \dots & G(C) \end{pmatrix}}_{l \text{ блоков}}, \quad (4)$$

где в каждой блочной строке $l - 1$ нулевых матриц $O_{k \times n}$ и одна матрица $G(C)$. Так как

$$\mathbb{F}_q^l \otimes C = \underbrace{C \times \dots \times C}_{l \text{ раз}},$$

то из леммы 2 вытекает

Следствие 1. Пусть C – $[n, k]$ -код с порождающей матрицей $G(C)$ и $\mathcal{W}(C)$ – нумератор кода C . Тогда

$$1) \mathcal{W}(\mathbb{F}_q^l \otimes C) = \underbrace{\mathcal{W}(C) \cdot \dots \cdot \mathcal{W}(C)}_{l \text{ раз}};$$

$$2) \forall i \in \{1, \dots, ln\} \exists j \in \{1, \dots, n\}: \mathcal{W}((\mathbb{F}_q^l \otimes C)_i) = \mathcal{W}(C_j) \cdot \underbrace{\mathcal{W}(C) \cdot \dots \cdot \mathcal{W}(C)}_{l-1 \text{ раз}}.$$

Также получаем, что проверочная матрица кода $\mathbb{F}_q^l \otimes C$ имеет вид $H(\mathbb{F}_q^l \otimes C) = E_l \otimes H(C)$, где $H(C)$ – проверочная матрица кода C , а из (3) следует, что остов кода $\mathbb{F}_q^l \otimes C$ имеет вид

$$\mathcal{H}(\mathbb{F}_q^l \otimes C) = \mathbb{F}_q^l \otimes \mathcal{H}(C). \quad (5)$$

Рассмотрим индуцированный код $\mathbb{F}_q^l \otimes C$, $l \in \mathbb{N}$. Группа автоморфизмов $\text{PAut}(\mathbb{F}_q^l \otimes C)$ этого кода нетривиальна. Действительно, порождающая матрица кода $\mathbb{F}_q^l \otimes C$ имеет блочно-диагональный вид (4) и при любой перестановке блоков этой матрицы получается порождающая матрица того же кода. Перестановка блочных столбцов этой матрицы эквивалентна перестановке блочных строк. Всего имеется $l!$ таких перестановок блочных столбцов. Поэтому мощность группы автоморфизмов кода $\mathbb{F}_q^l \otimes C$ не менее $l!$. Отсюда справедлива следующая

Лемма 3. Группа автоморфизмов $\text{PAut}(\mathbb{F}_q^l \otimes C)$ кода $\mathbb{F}_q^l \otimes C$ содержит подгруппу $\mathcal{G}(\mathbb{F}_q^l \otimes C)$, изоморфную группе S_l .

Отметим, что каждый элемент группы $\mathcal{G}(\mathbb{F}_q^l \otimes C)$ имеет вид

$$\left(\begin{array}{cccccc} 1 & \dots & n & \dots & (l-1)n+1 & \dots & ln \\ (\sigma(1)-1)n+1 & \dots & \sigma(1)n & \dots & (\sigma(l)-1)n+1 & \dots & \sigma(l)n \end{array} \right), \quad \sigma \in S_l. \quad (6)$$

Пусть $I_{i,n} = \{i, i+n, \dots, i+(l-1) \cdot n\}$, где $i \in \{1, \dots, n\}$, $S(I_{i,n})$ – подгруппа группы S_{ln} , перестановки из которой переставляют только элементы множества $I_{i,n}$, а элементы из множества $\{1, \dots, ln\} \setminus I_{i,n}$ оставляют на месте. Рассмотрим группу $Q = S(I_{1,n}) \times S(I_{2,n}) \times \dots \times S(I_{n,n}) \subset S_{ln}$, $|Q| = (l!)^n$. Несложно проверить, что

$$\mathcal{G}(\mathbb{F}_q^l \otimes C) \subseteq \text{PAut}(\mathbb{F}_q^l \otimes C) \cap Q. \quad (7)$$

Напомним, что орбитой элемента $i \in \{1, \dots, ln\}$ под действием подгруппы $\mathcal{G} \subseteq S_{ln}$ называется множество $\{g(i) : g \in \mathcal{G}\}$. Тогда $I_{i,n}$, $i = 1, \dots, n$, – это орбиты, образующиеся под действием подгруппы $\mathcal{G}(\mathbb{F}_q^l \otimes C)$ на элементах множества $\{1, \dots, ln\}$. Из (7) вытекает следующая вспомогательная

Лемма 4. Длина каждой орбиты, образующейся под действием группы $\text{PAut}(\mathbb{F}_q^l \otimes C)$ на элементы множества $\{1, \dots, ln\}$, кратна l .

2.3. Алгоритм расщепления носителя

Выше было отмечено, что для двух перестановочно-эквивалентных кодов с полным дискриминантом $\mathcal{S}$ для нахождения подходящей перестановки потребуется не более одной итерации внутреннего цикла алгоритма SSA. Из леммы 3 следует, что для кода $\mathbb{F}_q^l \otimes C$ не существует полного дискриминанта, так как группа автоморфизмов этого кода нетривиальна. Рассмотрим задачу построения для кодов $\mathbb{F}_q^l \otimes C$ и $D = \sigma(\mathbb{F}_q^l \otimes C)$ алгоритма нахождения такой подходящей перестановки σ' , что $\sigma'(\mathbb{F}_q^l \otimes C) = D$.

Лемма 5. Пусть C – $[n, k, d]$ -код. Тогда для $i = 1, \dots, n$ и любой сигнатуры $\mathcal{S}$, определенной по правилу (1), имеет место равенство

$$\mathcal{S}(\mathbb{F}_q^2 \otimes C, i) = \mathcal{S}(\mathbb{F}_q^2 \otimes C, i + n). \quad (8)$$

Доказательство. По определению (1), $\mathcal{S}(\mathbb{F}_q^2 \otimes C, i) = \mathcal{V}((\mathbb{F}_q^2 \otimes C)_i)$. Пусть $\mathcal{V}((\mathbb{F}_q^2 \otimes C)_i) \neq \mathcal{V}((\mathbb{F}_q^2 \otimes C)_{i+n})$. Для любой перестановки π из определения инварианта получаем: $\mathcal{V}((\mathbb{F}_q^2 \otimes C)_i) = \mathcal{V}(\pi((\mathbb{F}_q^2 \otimes C)_i))$. Рассмотрим произвольную нетривиальную перестановку $\pi \in \mathcal{G}(\mathbb{F}_q^2 \otimes C)$. Получаем

$$\mathcal{V}((\mathbb{F}_q^2 \otimes C)_i) = \mathcal{V}(\pi((\mathbb{F}_q^2 \otimes C)_i)) = \mathcal{V}(\pi(\mathbb{F}_q^2 \otimes C)_{\pi(i)}) = \mathcal{V}((\mathbb{F}_q^2 \otimes C)_{\pi(i)}).$$

Так как π — нетривиальная перестановка, то из вида (6) элементов группы $\mathcal{G}(\mathbb{F}_q^2 \otimes C)$ для $l = 2$ получим: $\pi(i) = i + n$. Пришли к противоречию. $\square$

Учитывая представление (6), из леммы 5 вытекает

Следствие 2. Для кода $\mathbb{F}_q^l \otimes C$ и $i \in \{1, \dots, n\}$ имеем: $\mathcal{S}(\mathbb{F}_q^l \otimes C, i) = \mathcal{S}(\mathbb{F}_q^l \otimes C, i + n \cdot k)$, для всех $k = \{0, \dots, l - 1\}$.

Таким образом, любая сигнатура для кода $\mathbb{F}_q^l \otimes C$, определенная по правилу (1), имеет не более n различных значений. Заметим, что чем больше значений имеет сигнатура для кода, тем меньше в среднем потребуются циклов алгоритма SSA для нахождения подходящей перестановки.

Лемма 6. Если $\mathcal{G}(\mathbb{F}_q^l \otimes C) \subset \text{PAut}(\mathbb{F}_q^l \otimes C)$, то любая сигнатура для кода C , определенная по правилу (1), имеет менее n значений.

Доказательство. Из следствия 2 получаем, что любая сигнатура для кода $\mathbb{F}_q^l \otimes C$, определенная по правилу (1), имеет не более n различных значений. Отсюда и из утверждения 8 работы [8] следует, что под действием группы $\text{PAut}(\mathbb{F}_q^l \otimes C)$ на множестве $\{1, \dots, ln\}$ образуется не более n различных орбит. Пусть $\sigma \in \text{PAut}(\mathbb{F}_q^l \otimes C) \setminus \mathcal{G}(\mathbb{F}_q^l \otimes C)$, тогда существует такой элемент $i \in \{1, \dots, n\}$, что $\sigma(i) \neq i + n \cdot k$ для некоторого $k \in \{0, \dots, l - 1\}$. Поэтому из леммы 4 получаем, что, как минимум, одна из орбит имеет длину не менее $2l$. Следовательно, под действием группы $\text{PAut}(\mathbb{F}_q^l \otimes C)$ образуется не более $n - 1$ орбит. Из утверждения 8 работы [8] получаем, что сигнатура имеет не более $n - 1$ различных значений. $\square$

Следствие 3. Пусть сигнатура $\mathcal{S}$ определена в соответствии с правилом (1). Если $\mathcal{S}$ для кода $\mathbb{F}_q^l \otimes C$ имеет n различных значений, то $\text{PAut}(\mathbb{F}_q^l \otimes C) = \mathcal{G}(\mathbb{F}_q^l \otimes C)$.

Пример 1. Рассмотрим код $C^1 \times C^2$ и найдем нумератор весов кода $(C^1 \times C^2)_i$, когда $i \in \{1, \dots, n_1 + n_2\}$. Если $i \leq n_1$, то $\mathcal{W}((C^1 \times C^2)_i) = \mathcal{W}(C_i^1) \cdot \mathcal{W}(C^2)$; если $n_1 < i \leq n_1 + n_2$, то $\mathcal{W}((C^1 \times C^2)_i) = \mathcal{W}(C^1) \cdot \mathcal{W}(C_{i-n_1}^2)$. Тогда

$$\mathcal{S}^W(C^1 \times C^2, i) = \mathcal{W}((C^1 \times C^2)_i) = \mathcal{W}(C_{i-(a-1) \cdot n_1}^a) \cdot \mathcal{W}(C^b), \quad (9)$$

где

$$a = \begin{cases} 1, & \text{при } 1 \leq i \leq n_1 \\ 2, & \text{при } n_1 + 1 \leq i \leq n_1 + n_2 \end{cases},$$

$b = \{1, 2\} \setminus \{a\}$. В случае $C^1 = C^2 = C$ получаем: $C^1 \times C^2 = \mathbb{F}_q^2 \otimes C$, поэтому

$$\mathcal{S}^W(\mathbb{F}_q^2 \otimes C, i) = \mathcal{W}(C) \cdot \mathcal{W}(C_j), \quad (10)$$

где

$$j = \begin{cases} i, & \text{при } 1 \leq i \leq n \\ i - n, & \text{при } n < i \leq 2n. \end{cases}$$

Если C — такой $[n, k]$ -код, что $\mathcal{S}^W$ — его полный дискриминант, то, как непосредственно вытекает из следствия 1 и из обобщения формулы (10) на случай $l \geq 2$, сигнатура $\mathcal{S}^W$ для кода $\mathbb{F}_q^l \otimes C$ имеет n различных значений. Из следствия 3 тогда вытекает, что в этом случае группа автоморфизмов кода $\mathbb{F}_q^l \otimes C$ имеет простое описание.

Лемма 7. Пусть $\mathcal{S}$ — сигнатура, определенная по правилу (1). Тогда для любого $\pi \in Q$ выполняются равенства:

- 1) $\mathcal{S}(\mathbb{F}_q^l \otimes C, i) = \mathcal{S}(\mathbb{F}_q^l \otimes C, \pi(i))$, $i = 1, \dots, ln$;
- 2) $(\mathcal{S}(\mathbb{F}_q^l \otimes C, i))_{i=1}^{ln} = (\mathcal{S}(\mathbb{F}_q^l \otimes C, \pi(i)))_{i=1}^{ln}$;
- 3) $(\mathcal{S}(\mathbb{F}_q^l \otimes C, i))_{i=1}^{ln} = \pi((\mathcal{S}(\mathbb{F}_q^l \otimes C, i))_{i=1}^{ln})$.

Доказательство. Доказательство равенства 1) вытекает из следствия 2; равенство 2) следует из 1). Докажем утверждение 3). Из 2) следует

$$\begin{aligned} (\mathcal{S}(\mathbb{F}_q^l \otimes C, i))_{i=1}^{ln} &= (\mathcal{S}(\mathbb{F}_q^l \otimes C, \pi(i)))_{i=1}^{ln} \\ &= (\mathcal{S}(\mathbb{F}_q^l \otimes C, j))_{\pi^{-1}(j)=1}^{ln} = \pi((\mathcal{S}(\mathbb{F}_q^l \otimes C, j))_{j=1}^{ln}). \end{aligned}$$

Так как π — произвольная перестановка из группы Q , то утверждение доказано. $\square$

Символом σQ обозначим фактор-класс $\{\sigma\pi : \pi \in Q\}$ фактор-множества S_{nl}/Q .

Лемма 8. Если сигнатура $\mathcal{S}$ для кода $\mathbb{F}_q^l \otimes C$ определена по правилу (1) и имеет n различных значений, $D = \sigma(\mathbb{F}_q^l \otimes C)$ и

$$(\mathcal{S}(D, i))_{i=1}^{ln} = \gamma((\mathcal{S}(\mathbb{F}_q^l \otimes C, i))_{i=1}^{ln}), \quad (11)$$

то $\sigma \in \gamma Q$.

Доказательство. Из утверждения 3) леммы 7 и условия (11) получаем, что для любого $\pi \in Q$ выполняются равенства

$$(\mathcal{S}(D, i))_{i=1}^{ln} = \gamma((\mathcal{S}(\mathbb{F}_q^l \otimes C, i))_{i=1}^{ln}) = \gamma\pi((\mathcal{S}(\mathbb{F}_q^l \otimes C, i))_{i=1}^{ln}).$$

Так как, по условию, сигнатура имеет максимальное количество различных значений — n , то $\sigma \in \gamma Q$ по построению группы Q (Q — максимальная в этом случае подгруппа, не меняющая порядка элементов в наборе $(\mathcal{S}(\mathbb{F}_q^l \otimes C, i))_{i=1}^{ln}$). $\square$

Пусть $Q/\mathcal{G}(\mathbb{F}_q^l \otimes C) = \{G_i\}_{i=0}^x$ — фактор-множество группы Q по подгруппе $\mathcal{G}(\mathbb{F}_q^l \otimes C)$, $x+1 = |Q|/|\mathcal{G}(\mathbb{F}_q^l \otimes C)| = (ln)^n/ln = (ln)^{n-1}$. Пусть также $\Omega = \{\omega_0, \dots, \omega_x\}$ — трансверсаль фактор-множества $Q/\mathcal{G}(\mathbb{F}_q^l \otimes C)$, или множество представителей классов смежности, $G_i = \omega_i \mathcal{G}(\mathbb{F}_q^l \otimes C)$, $i = 0, \dots, x$. Одним из возможных алгоритмов построения множества Q является алгоритм MakeRepresentatives.

Исходные параметры: $Q, \mathcal{G}(\mathbb{F}_q^l \otimes C)$

Результат: Ω — множество представителей классов фактор-множества $Q/\mathcal{G}(\mathbb{F}_q^l \otimes C)$

1. $\Omega = \emptyset$
 2. **до тех пор, пока** $|\Omega| < (l!)^{n-1}$ **выполнять**

Случайно сгенерировать перестановку $\pi' \in Q$ если $\pi' \notin \mathcal{G}(\mathbb{F}_q^l \otimes C)$ и $\pi'^{-1}\sigma \notin \mathcal{G}(\mathbb{F}_q^l \otimes C) \forall \sigma \in \Omega$ тогда $\Omega = \Omega \cup \{\pi'\}$ конец условия

- конец цикла**
возвратить Ω

Алгоритм 2: MakeRepresentatives

Теорема 1. Пусть C — $[n, k]$ -код, $D = \sigma(\mathbb{F}_q^l \otimes C)$, $\mathcal{S}$ — сигнатура, определенная по правилу (1) и имеющая n различных значений для кода $\mathbb{F}_q^l \otimes C$, Ω — трансверсаль фактор-множества $Q/\mathcal{G}(\mathbb{F}_q^l \otimes C)$. Тогда существует алгоритм с вычислительной сложностью $\mathcal{O}(|\Omega|)$, который находит подходящую перестановку σ' такую, что $D = \sigma'(\mathbb{F}_q^l \otimes C)$.

Доказательство. Пусть $(\mathcal{S}(D, i))_{i=1}^{ln} = \gamma((\mathcal{S}(\mathbb{F}_q^l \otimes C, i))_{i=1}^{ln})$. Такая перестановка γ может быть найдена простым вычислением сигнатур кодов D и C . Тогда из леммы 8 получаем, что $\sigma \in \gamma Q$. Из леммы 1 видим, что подходящей перестановкой, переводящей код $\mathbb{F}_q^l \otimes C$ в код D , является перестановка вида $\sigma\pi$, где $\pi \in \text{PAut}(\mathbb{F}_q^l \otimes C)$. Так как сигнатура имеет n различных значений, то из следствия 3 получаем, что $\text{PAut}(\mathbb{F}_q^l \otimes C) = \mathcal{G}(\mathbb{F}_q^l \otimes C)$. Отсюда получаем, что подходящая перестановка может быть найдена путем перебора элементов трансверсали Ω . Таким образом, для нахождения подходящей перестановки достаточно выполнить алгоритм SSAForTensor, сложность которого $\mathcal{O}(|\Omega|)$, так как в этом алгоритме осуществляется перебор по трансверсали Ω . $\square$

Исходные параметры: $\mathbb{F}_q^l \otimes C \in \mathcal{L}_{ln}$, $D = \sigma(\mathbb{F}_q^l \otimes C)$, $\mathcal{S}, \Omega$

Результат: $\sigma' : \sigma'(\mathbb{F}_q^l \otimes C) = D$

1. Вычислить $\mathcal{D} = (\mathcal{S}(D, i))_{i=1}^{ln}$.
 2. Вычислить $\mathcal{C} = (\mathcal{S}(\mathbb{F}_q^l \otimes C, i))_{i=1}^{ln}$.
 3. Найти подходящую перестановку γ такую, что $\gamma(\mathcal{C}) = \mathcal{D}$.
 4. **для каждого** $\omega \in \Omega$ **выполнять**

если $(\gamma\omega)^{-1}(D) = \mathbb{F}_q^l \otimes C$ тогда $\sigma' = \gamma\omega$ выход конец условия
--
- конец цикла**
возвратить σ'

Алгоритм 3: SSAForTensor

Отметим, что в теореме 1 при оценке сложности алгоритма SSAForTensor учитывается только мощность трансверсали, но не учитывается сложность вычисления

сигнатур (шаги 1 и 2), сложность проверки совпадения двух кодов (шаг 4), а также сложность построения трансверсали Ω , используемой в качестве входного параметра. Совпадение двух кодов можно проверить, умножив порождающую матрицу кода $(\gamma\omega)^{-1}(D)$ на проверочную матрицу $H(\mathbb{F}_q^l \otimes C)$ кода $\mathbb{F}_q^l \otimes C$. Таким образом, сложность этой проверки полиномиально зависит от ln , т.е. эта проверка может быть выполнена эффективным способом. В то же время построение эффективно вычисляемых сигнатур является отдельной задачей [8]. В частности, в [8] для построения эффективных сигнатур применяется нумератор остова кода, который с большой вероятностью имеет малую размерность. Из (5) следует, что размерность остова для индуцированного кода увеличивается в l раз по сравнению с остовом базового кода. Это в свою очередь может существенно замедлить подсчет нумераторов его проекций в общем случае и усложнит вычисление сигнатур, так как для вычисления нужно перебрать все векторы проекции остова для всех координат. Построение трансверсали Ω также представляется сложной задачей при достаточно больших значениях ln . Например, предложенный алгоритм MakeRepresentatives имеет неполиномиальную от ln сложность, хотя и может выполняться заранее.

Тем не менее, если для кода $\mathbb{F}_q^l \otimes C$ имеется эффективно вычисляемая сигнатура, определенная по правилу (1) и имеющая n различных значений, а также имеется трансверсаль Ω , то при нахождении подходящей перестановки алгоритм SSAForTensor будет эффективнее алгоритма SSA. Это обусловлено тем, что алгоритм SSA выполняет поиск подходящей перестановки по всему классу смежности σQ , а алгоритм SSAForTensor выполняет поиск только по множеству $\sigma\Omega$, мощность которого в $l!$ меньше $|\sigma Q|$, так как $|Q|/|\Omega| = |\mathcal{G}(\mathbb{F}_q^l \otimes C)| = l!$.

3. Применение индуцированных кодов в криптографии

3.1. Криптосистема типа Мак-Элиса на основе индуцированных кодов

Рассмотрим криптосистему типа Мак-Элиса на основе $[ln, lk, d]$ -кода $\mathbb{F}_q^l \otimes C$, где C — $[n, k, d]$ -код с порождающей матрицей $G(C)$. В этой криптосистеме открытый ключ $\mathbf{k}_{\text{pub}}$ — это пара $(\tilde{G}, t = \lfloor (d-1)/2 \rfloor)$, а секретный ключ $\mathbf{k}_{\text{sec}}$ — пара матриц (S, P) , где S — случайная невырожденная $(lk \times lk)$ -матрица, P — случайная перестановочная $(ln \times ln)$ -матрица, причем $\tilde{G} = S \cdot (E_l \otimes G(C)) \cdot P$, где E_l — единичная матрица размера $l \times l$. Правило шифрования произвольного сообщения $\mathbf{s} \in \mathbb{F}_q^{lk}$ имеет вид

$$\mathbf{z} = \mathbf{s}\tilde{G} + \mathbf{e}, \quad (12)$$

где $\mathbf{e} \in \mathbb{F}_q^{ln}$ и $\text{wt}(\mathbf{e}) \leq t$.

При расшифровании используется правило $\mathbf{s} = \text{Dec}_C(\mathbf{z}P^{-1})S^{-1}$, где $\text{Dec}_{\mathbb{F}_q^l \otimes C} : \mathbb{F}_q^{ln} \rightarrow \mathbb{F}_q^{lk}$ — декодер кода $\mathbb{F}_q^l \otimes C$, гарантированно исправляющий t и менее ошибок и восстанавливающий вектор $\mathbf{s}$. Криптосистему Мак-Элиса на коде $\mathbb{F}_q^l \otimes C$ обозначим $\text{McE}(\mathbb{F}_q^l \otimes C)$.

Так как код с порождающей матрицей $\tilde{G}$ и код $\mathbb{F}_q^l \otimes C$ являются перестановочно-эквивалентными, то, как следует, например, из [4], для взлома $\text{McE}(\mathbb{F}_q^l \otimes C)$, достаточно найти такую пару матриц (S', P') , что $S'(E_l \otimes G(C))P' = \tilde{G}$ и перестановка, соответствующая перестановочной матрице $P'^{-1}P$, принадлежит $\text{PAut}(\mathbb{F}_q^l \otimes C)$.

В [7] показано, что если криптосистема Мак-Элиса $\text{McE}(C)$ на основе базового кода C является нестойкой к атакам на ключ, то существует алгоритм нахождения подходящей перестановочной матрицы (подходящей перестановки) для криптосистемы $\text{McE}(\mathbb{F}_q^l \otimes C)$, сложность выполнения которого оценивается величиной $\mathcal{O}(\frac{(nl)!}{(n!)^l l!})$. По формуле Стирлинга получаем, что

$$\frac{(nl)!}{(n!)^l l!} \approx \frac{\sqrt{2\pi nl} (\frac{n}{e})^{nl}}{(\sqrt{2\pi n} (\frac{n}{e})^n)^l \sqrt{2\pi l} (\frac{l}{e})^l} = \sqrt{\frac{n}{(2\pi n)^l}} \cdot e^l \cdot l^{l(n-1)}. \quad (13)$$

Кроме того, для нахождения подходящей перестановки, в случае существования дискриминанта для кода $\mathbb{F}_q^l \otimes C$, может быть применен алгоритм SSA. Рассмотрим наиболее выгодные, с точки зрения атакующего, условия, когда для кода $\mathbb{F}_q^l \otimes C$ известна эффективно вычисляемая сигнатура $\mathcal{S}$, имеющая n различных значений для кода $\mathbb{F}_q^l \otimes C$, а также построена трансверсаль Ω фактор-множества $Q/\mathcal{G}(\mathbb{F}_q^l \otimes C)$. Таким образом, выполняются условия теоремы 1, и поэтому вместо алгоритма SSA атакующим может быть применен алгоритм SSAForTensor. Из теоремы 1 получаем, что стойкость криптосистемы $\text{McE}(\mathbb{F}_q^l \otimes C)$ оценивается величиной $\mathcal{O}(|\Omega|) = \mathcal{O}((l!)^{n-1})$. Используя формулу Стирлинга, получаем

$$(l!)^{n-1} \approx \left(\sqrt{2\pi l} \left(\frac{l}{e} \right)^l \right)^{n-1} = \left(\frac{\sqrt{2\pi l}}{e^l} \right)^{n-1} \cdot l^{l(n-1)}. \quad (14)$$

Заметим, что (13) и (14) — это оценки на мощности множеств ключей, по которым перебором осуществляется поиск подходящих перестановок соответственно алгоритмом из [7] и алгоритмом SSAForTensor. В настоящее время, согласно [10], считается вычислительно не осуществимым перебор по ключевому множеству мощности 2^{128} и более. Для наглядного сравнения оценок (13) и (14) рассмотрим пример, когда для построения индуцированного кода $\mathbb{F}_q^l \otimes C$ используется двоичный $[n, k, d]$ -код C Рида–Маллера, $n \in \{8, 16, 32, 64, 128, 256\}$, $q = 2$.

В таблицах 2 и 1 приведены результаты вычисления величины $\log_2 K$ для атаки на криптосистему $\text{McE}(\mathbb{F}_2^l \otimes C)$, $l \in \{2, 3, 4, 5, 6, 7, 8, 9\}$, где для таблицы 1 значение K вычисляется в соответствии с (13), а для таблицы 2 — в соответствии с (14). В таблицах 1 и 2 выделены ячейки, соответствующие тем параметрам индуцированного кода $\mathbb{F}_2^l \otimes C$, для которых сложность перебора не менее 2^{128} . Сравнение соответствующих значений из таблиц показывает, что атака на основе алгоритма расщепления носителя SSAForTensor существенно эффективнее атаки, описанной в [7], однако при подборе параметров n и l эта атака может быть также неосуществимой.

В [11] показано, что применение индуцированных кодов в криптосистемах типа Мак-Элиса приводит к ослаблению стойкости этой системы к атакам на шифrogramму на основе метода декодирования по информационным совокупностям. Приемлемая стойкость к таким атакам достигается при больших длинах кода. Это связано с тем, что размерность и длина индуцированных кодов увеличиваются в l раз,

Таблица 1. Значения величины $\log_2\left(\frac{(nl)!}{(n!)^l l!}\right)$.

Table 1. Values of $\log_2\left(\frac{(nl)!}{(n!)^l l!}\right)$.

l / n	8	16	32	64	128	256
2	12.73	28.23	59.73	123.23	250.73	506.23
3	30.63	67.67	142.75	293.90	597.22	>1024
4	51.96	114.46	240.96	495.46	1006	>1024
5	75.85	166.72	350.48	719.99	>1024	>1024
6	101.77	223.34	469	962.81	>1024	>1024
7	129.37	283.59	595.01	>1024	>1024	>1024
8	158.43	346.93	727.43	>1024	>1024	>1024
9	188.75	412.99	865.46	>1024	>1024	>1024

Таблица 2. Значения величины $\log_2(((l)!)^{n-1})$.

Table 2. Values of $\log_2(((l)!)^{n-1})$.

l / n	8	16	32	64	128	256
2	7	15	31	63	127	255
3	18.09	38.77	80.13	162.85	328.29	659.16
4	32.09	68.77	142.13	288.85	582.29	>1024
5	48.34	103.60	214.11	435.13	877.17	>1024
6	66.44	142.37	294.24	597.98	>1024	>1024
7	86.09	184.48	381.27	774.85	>1024	>1024
8	107.09	229.48	474.27	963.84	>1024	>1024
9	129.28	277.03	572.54	>1024	>1024	>1024

однако кодовое расстояние не меняется. Тем не менее, применение криптосистемы $\text{McE}(\mathbb{F}_2^l \otimes C)$ возможно в тех случаях, когда при шифровании добавляются векторы ошибок веса, большего, чем может исправить декодер $\text{Dec}_{\mathbb{F}_2^l \otimes C}$. Например, в [7] предложен протокол выработки общего секретного ключа на основе построенной криптосистемы. В следующем подразделе предлагается еще одно применение индуцированных кодов: применение в криптографических протоколах идентификации.

3.2. Протокол идентификации на основе индуцированных кодов

В [12] М. Жиро построил протокол идентификации на основе сложности нахождения перестановки для двух перестановочно-эквивалентных кодов над бинарным полем. Приведем этот протокол для случая $\mathbb{F}_q$. Пусть H — это $(N - K \times N)$ -матрица над полем $\mathbb{F}_q$, общая для всех пользователей протокола. Каждый пользователь $\mathcal{P}$

выбирает случайно вектор $\mathbf{e}$ небольшого веса w и вычисляет $H\mathbf{e}^\top = \mathbf{s}^\top$. Вектор $\mathbf{s}$ является публичным идентификатором пользователя $\mathcal{P}$. В случае, когда проверяющая сторона $\mathcal{V}$ намерена провести аутентификацию пользователя $\mathcal{P}$, то есть проверить, что аутентифицируемый пользователь знает вектор $\mathbf{e}$, выполняется 3-шаговый протокол.

Шаг 1: $\mathcal{P}$ случайно и равновероятно выбирает перестановочную $(N \times N)$ -матрицу P и невырожденную $(N - K \times N - K)$ -матрицу S , вычисляет $\tilde{H} = SHP$, $\mathbf{s}' = S\mathbf{s}$ и отправляет $\mathcal{V}$ матрицу $\tilde{H}$ и вектор $\mathbf{s}'$.

Шаг 2: $\mathcal{V}$ случайно и равновероятно выбирает бит $c \in \{0, 1\}$ и посылает его $\mathcal{P}$.

Шаг 3а: Если $c = 0$, то $\mathcal{P}$ передает матрицы S и P стороне $\mathcal{V}$, которая проверяет, что $SHP = \tilde{H}$ и $\mathbf{s}' = S\mathbf{s}$.

Шаг 3б: Если $c = 1$, то $\mathcal{P}$ передает $\mathbf{e}' = P^{-1}\mathbf{e}$ стороне $\mathcal{V}$, которая проверяет, что $\text{wt}(\mathbf{e}') = w$ и $\tilde{H}\mathbf{e}' = \mathbf{s}$.

Этот протокол выполняется m раз, где параметр безопасности m выбирается так, чтобы вероятность $1/2^m$ мошенничества доказывающей стороны была менее наперед заданного порога. Оценим коммуникационную сложность этого протокола. На Шаге 1 доказывающая сторона передает $(N - K)(N + 1) \log_2 q$ бит данных. На втором шаге проверяющая сторона передает один бит. Количество передаваемых данных на Шаге 3 зависит от значения бита c : при $c = 0$ передается $(N - K)^2 \log_2 q + N \log_2 N$ бит, а при $c = 1$ передается $N \log_2 q$ бит. Учитывая, что значение бита c выбирается случайно и равновероятно, то в среднем за m итераций коммуникационная сложность протокола составит

$$\left(1 + \frac{3N - K}{2}\right) m(N - K) \log_2 q + N(\log_2 N + m/2 \log_2 q) + m \text{ бит.} \quad (15)$$

В [13] отмечено, что если матрица H выбирается случайно, то протокол Жиро не является стойким. В то же время отмечено, что возможно применение кодов, для которых осто́в имеет большую размерность, так как сложность вычисления сигнатуры $\mathcal{S}^W$, предложенной в [8], зависит нелинейно от размерности осто́ва. К таким кодам, например, относятся индуцированные коды вида $\mathbb{F}_q^l \otimes C$, так как размерность осто́ва таких кодов, как следует из (5), в l раз больше размерности осто́ва базового кода C . Если не учитывать сложность вычисления сигнатуры (т.е. полагать, что сигнатура вычисляется эффективно), то, как следует из таблицы 2, для реализации протокола Жиро может быть использован такой код $\mathbb{F}_q^l \otimes C$ на основе кода Рида–Маллера, для которого значение ячейки в таблице 2 больше 128. Учитывая, что коммуникационная сложность (15) растет с ростом $N = ln$, следует выбирать те параметры индуцированного кода, для которого ln принимает наименьшее из допустимых значений. В рассмотренном в предыдущем подразделе примере минимально допустимое значение ln равно $72 = 9 \cdot 8$.

Список литературы / References

- [1] McEliece R. J., “A Public-Key Cryptosystem Based on Algebraic Coding Theory”, *JPL Deep Space Network Progress Report*, 1978, № 42–44, 114–116.
 - [2] Sendrier N., Tillich J. P., *Code-Based Cryptography: New Security Solutions Against a Quantum Adversary*, ERCIM News, ERCIM, 2016 <https://hal.archives-ouvertes.fr/hal-01410068/document>.
 - [3] Morelos-Zaragoza R. H., *The Art of Error Correcting Coding*, 2nd Edition, John Wiley & Sons, Inc., 2006.
 - [4] Sidel’nikov V. M., Shestakov S. O., “On an encoding system constructed on the basis of generalized Reed-Solomon codes”, *Discrete Mathematics and Applications*, **2**:4 (1992), 439–444.
 - [5] Бородин М. А., Чижов И. В., “Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида-Маллера”, *Дискрет. матем.*, **26**:1 (2014), 10–20; English transl.: Borodin M. A., Chizhov I. V., “Effective attack on the McEliece cryptosystem based on Reed-Muller codes”, *Discrete Mathematics and Applications*, **24**:5 (2014), 273–280.
 - [6] Деундяк В. М., Косолапов Ю. В., “Алгоритмы для мажоритарного декодирования групповых кодов”, *Модел. и анализ информ. систем*, **22**:4 (2015), 464–482; [Deundyak V. M., Kosolapov Yu. V., “Algorithms for majority decoding of group codes”, *Model. Anal. Inform. Sist.*, **22**:4 (2015), 464–482, (in Russian).]
 - [7] Деундяк В. М., Косолапов Ю. В., “Криптосистема на индуцированных групповых кодах”, *Модел. и анализ информ. систем*, **23**:2 (2016), 137–152; [Deundyak V. M., Kosolapov Yu. V., “Cryptosystem based on induced group codes”, *Model. Anal. Inform. Sist.*, **23**:2 (2016), 137–152, (in Russian).]
 - [8] Sendrier N., “Finding the Permutation Between Equivalent Linear Codes: The Support Splitting Algorithm”, *IEEE Trans. on IT*, **46**:4 (2000), 1193–1203.
 - [9] Haily A., Harzalla D., “On Binary Linear Codes Whose Automorphism Group is Trivial”, *Journal of Discrete Mathematical Sciences and Cryptography*, **18**:5 (2015), 495–512.
 - [10] Lenstra A. K., Verheul E. R., “Selecting Cryptographic Key Sizes”, *Journal of Cryptology*, **14**:4 (2001), 255–293.
 - [11] Деундяк В. М., Косолапов Ю. В., “Использование тензорного произведения кодов Рида-Маллера в асимметричной криптосистеме типа Мак-Элиса и анализ ее стойкости к атакам на шифrogramму”, *Вычислительные технологии*, **22**:4 (2017), 43–60; [Deundyak V. M., Kosolapov Yu. V., “The use of the tensor product of Reed-Muller codes in asymmetric McEliece type cryptosystem and analysis of its resistance to attacks on the cryptogram”, *Computational Technologies*, **22**:4 (2017), 43–60, (in Russian).]
 - [12] Girault M., “A (non-practical) three-pass identification protocol using coding theory”, *Advances in Cryptology AUSCRYPT ’90*, Lecture Notes in Computer Science, **453**, 1990, 265–272.
 - [13] Sendrier N., Simos D. E., “The Hardness of Code Equivalence over $\mathbb{F}_q$ and its Application to Code-based Cryptography”, *Post-Quantum Cryptography. PQCrypto 2013*, Lecture Notes in Computer Science, **7932**, 2013, 203–216.
-

Kosolapov Yu. V., Shigaev A. N., "The Support Splitting Algorithm for Induced Codes", *Modeling and Analysis of Information Systems*, **25**:3 (2018), 276–290.

DOI: 10.18255/1818-1015-2018-3-276-290

Abstract. In the paper, the analysis of the stability of the McEliece-type cryptosystem on induced codes for key attacks is examined. In particular, a model is considered when the automorphism group is trivial for the base code C , on the basis of which the induced code $\mathbb{F}_q^l \otimes C$ is constructed. In this case, as shown by N. Sendrier in 2000, there exists such a mapping, called a complete discriminant, by means of which a secret permutation that is part of the secret key of a McEliece-type cryptosystem can be effectively found. The automorphism group of the code $\mathbb{F}_q^l \otimes C$ is nontrivial, therefore there is no complete discriminant for this code. This suggests a potentially high resistance of the McEliece-type cryptosystem on the code $\mathbb{F}_q^l \otimes C$. The algorithm for splitting the support for the code $\mathbb{F}_q^l \otimes C$ is constructed and the efficiency of this algorithm is compared with the existing attack on the key of the McEliece type cryptosystem based on the code $\mathbb{F}_q^l \otimes C$.

Keywords: group codes, induced group codes, support splitting algorithm, the McEliece cryptosystem

On the authors:

Yury V. Kosolapov, orcid.org/0000-0002-1491-524X, PhD,
South Federal University, 105/42 Bolshaya Sadovaya Str., Rostov-on-Don, 344006, Russia, e-mail: itaim@mail.ru

Aleksey N. Shigaev, orcid.org/0000-0001-6363-4332, graduate student,
South Federal University, 105/42 Bolshaya Sadovaya Str., Rostov-on-Don, 344006, Russia, e-mail: aleksejshig@gmail.com

Вычислительная геометрия

©Невский М. В., Ухалов А. Ю., 2017

DOI: 10.18255/1818-1015-2018-3-291-311

УДК 514.17+517.51+519.6

Об оптимальной интерполяции линейными функциями на n -мерном кубе

Невский М. В., Ухалов А. Ю.

получена 11 декабря 2017

Аннотация. Пусть $n \in \mathbb{N}$, $Q_n = [0, 1]^n$. Через $C(Q_n)$ обозначим пространство непрерывных функций $f : Q_n \rightarrow \mathbb{R}$ с нормой $\|f\|_{C(Q_n)} := \max_{x \in Q_n} |f(x)|$, через $\Pi_1(\mathbb{R}^n)$ — совокупность многочленов от n переменных степени ≤ 1 (или линейных функций). Пусть $x^{(j)}$, $1 \leq j \leq n+1$, — вершины n -мерного невырожденного симплекса $S \subset Q_n$. Интерполяционный проектор $P : C(Q_n) \rightarrow \Pi_1(\mathbb{R}^n)$, соответствующий симплексу S , определяется равенствами $Pf(x^{(j)}) = f(x^{(j)})$. Норма P как оператора из $C(Q_n)$ в $C(Q_n)$ может быть вычислена по формуле $\|P\| = \max_{x \in \text{ver}(Q_n)} \sum_{j=1}^{n+1} |\lambda_j(x)|$. Здесь λ_j — базисные многочлены Лагранжа, соответствующие S , $\text{ver}(Q_n)$ — совокупность вершин Q_n . Через θ_n обозначим минимальную величину $\|P\|$. Ранее первым автором были доказаны различные соотношения и оценки для величин $\|P\|$ и θ_n , в том числе имеющие геометрический характер. Справедлива эквивалентность $\theta_n \asymp \sqrt{n}$. Подходящими по размерности n неравенствами являются, например, $\frac{1}{4}\sqrt{n} < \theta_n < 3\sqrt{n}$. Для проектора P^* , узлы которого совпадают с вершинами произвольного симплекса максимального объёма в кубе, выполняется $\|P^*\| \asymp \theta_n$. Если существует матрица Адамара порядка $n+1$, то $\theta_n \leq \sqrt{n+1}$. В настоящей статье приводятся уточнённые верхние границы чисел θ_n для $21 \leq n \leq 26$, полученные с применением симплексов максимального объёма в кубе. Для построения этих симплексов применяются максимальные определители, элементы которых равны ± 1 . Мы также систематизируем и комментируем лучшие на настоящий момент верхние и нижние оценки чисел θ_n для конкретных n .

Ключевые слова: n -мерный симплекс, n -мерный куб, интерполяция, проектор, норма, численные методы

Для цитирования: Невский М. В., Ухалов А. Ю., "Об оптимальной интерполяции линейными функциями на n -мерном кубе", *Моделирование и анализ информационных систем*, **25**:3 (2018), 291–311.

Об авторах:

Невский Михаил Викторович, orcid.org/0000-0002-6392-7618, д-р физ.-мат. наук, доцент, НОМЦ Центр интегрируемых систем, Ярославский государственный университет им. П.Г. Демидова, ул. Советская, 14, г. Ярославль, 150003 Российская Федерация, e-mail: mnevsk55@yandex.ru

Ухалов Алексей Юрьевич, orcid.org/0000-0001-6551-5118, кандидат физ.-мат. наук, НОМЦ Центр интегрируемых систем, Ярославский государственный университет им. П.Г. Демидова, ул. Советская, 14, г. Ярославль, 150003 Российская Федерация, e-mail: alex-uhalov@yandex.ru

Благодарности:

Работа выполнена в рамках государственного задания Министерства образования и науки РФ, проект № 1.12873.2018/12.1

1. Введение. Числа θ_n и ξ_n

В настоящей статье $n \in \mathbb{N}$, $Q_n := [0, 1]^n$. Через $C(Q_n)$ обозначается пространство непрерывных функций $f : Q_n \rightarrow \mathbb{R}$ с равномерной нормой $\|f\|_{C(Q_n)} := \max_{x \in Q_n} |f(x)|$.

Под $\Pi_1(\mathbb{R}^n)$ понимается совокупность многочленов от n переменных степени ≤ 1 , или линейных функций на $\mathbb{R}^n$. Запись $L(n) \asymp M(n)$ означает, что существуют $c_1, c_2 > 0$, не зависящие от n , с которыми выполняется $c_1 M(n) \leq L(n) \leq c_2 M(n)$. Соотношение $L(n) \cong M(n)$ означает, что $\lim_{n \rightarrow \infty} \frac{L(n)}{M(n)} = 1$. Для многогранника G через $\text{ver}(G)$ обозначается совокупность его вершин.

Пусть S — невырожденный симплекс в $\mathbb{R}^n$. Обозначим вершины S через $x^{(j)} = (x_1^{(j)}, \dots, x_n^{(j)})$, $1 \leq j \leq n+1$, и рассмотрим матрицу

$$\mathbf{A} := \begin{pmatrix} x_1^{(1)} & \dots & x_n^{(1)} & 1 \\ x_1^{(2)} & \dots & x_n^{(2)} & 1 \\ \vdots & \vdots & \vdots & \vdots \\ x_1^{(n+1)} & \dots & x_n^{(n+1)} & 1 \end{pmatrix}.$$

Пусть $\mathbf{A}^{-1} = (l_{ij})$. Обозначим через λ_j многочлен из $\Pi_1(\mathbb{R}^n)$, коэффициенты которого составляют j -й столбец $\mathbf{A}^{-1}$: $\lambda_j(x) = l_{1j}x_1 + \dots + l_{nj}x_n + l_{n+1,j}$. Мы называем λ_j базисными многочленами Лагранжа, соответствующими S . Числа $\lambda_j(x)$ являются барицентрическими координатами точки $x \in \mathbb{R}^n$ относительно S . Симплекс S задаётся каждой из систем неравенств $\lambda_j(x) \geq 0$ и $0 \leq \lambda_j(x) \leq 1$.

Через σS обозначим образ S при гомотетии относительно центра тяжести с коэффициентом σ . Под $d_i(S)$ будем понимать i -й осевой диаметр S , представляющий собой максимальную длину отрезка из S , параллельного i -й координатной оси. Понятие осевого диаметра выпуклого тела было введено Скоттом [23], [24].

Пусть $\xi(S) := \min\{\sigma \geq 1 : Q_n \subset \sigma S\}$, $\xi_n := \min\{\xi(S) : S \subset Q_n\}$. Через $\alpha(S)$ обозначим минимальное $\sigma > 0$, для которого Q_n принадлежит трансляту симплекса σS . Многие соотношения для этих величин были доказаны первым автором. В случае $Q_n \not\subset S$

$$\xi(S) = (n+1) \max_{1 \leq j \leq n+1} \max_{x \in \text{ver}(Q_n)} (-\lambda_j(x)) + 1. \quad (1)$$

Для любого S выполняются равенства

$$\alpha(S) = \sum_{i=1}^n \frac{1}{d_i(S)} = \frac{1}{2} \sum_{i=1}^n \sum_{j=1}^{n+1} |l_{ij}|. \quad (2)$$

(см. [22], [6]; доказательства даются также в [7]).

Всюду далее мы считаем, что $S \subset Q_n$. Интерполяционный проектор $P : C(Q_n) \rightarrow \Pi_1(\mathbb{R}^n)$, соответствующий симплексу S , определяется равенствами $Pf(x^{(j)}) = f(x^{(j)})$. Справедлив аналог интерполяционной формулы Лагранжа

$$Pf(x) = \sum_{j=1}^{n+1} f(x^{(j)}) \lambda_j(x).$$

Норма проектора P как оператора из $C(Q_n)$ в $C(Q_n)$ вычисляется по формуле

$$\|P\| = \max_{x \in \text{ver}(Q_n)} \sum_{j=1}^{n+1} |\lambda_j(x)|. \quad (3)$$

Через θ_n обозначим минимальную величину $\|P\|$. Под θ'_n понимается минимальная величина нормы проектора, узлы которого находятся в вершинах Q_n . Очевидно, $\theta_n \leq \theta'_n$.

Пусть $1 \leq \mu \leq n$. Будем говорить, что точка $x \in \text{ver}(Q_n)$ является μ -вершиной куба Q_n относительно симплекса S , если для проектора $P : C(Q_n) \rightarrow \Pi_1(\mathbb{R}^n)$ с узлами в вершинах S выполняется $\|P\| = \sum_{j=1}^{n+1} |\lambda_j(x)|$ и среди чисел $\lambda_j(x)$ имеется ровно μ отрицательных. Для любого проектора P и соответствующего ему симплекса S в [5] установлено соотношение

$$\frac{n+1}{2n} (\|P\| - 1) + 1 \leq \xi(S) \leq \frac{n+1}{2} (\|P\| - 1) + 1. \quad (4)$$

Правое равенство имеет место тогда и только тогда, когда существует 1-вершина Q_n относительно S . Если для некоторого μ имеется μ -вершина Q_n относительно S , то $\frac{n+1}{2\mu} (\|P\| - 1) + 1 \leq \xi(S)$. Из (4) следует, что

$$\frac{n+1}{2n} (\theta_n - 1) + 1 \leq \xi_n \leq \frac{n+1}{2} (\theta_n - 1) + 1. \quad (5)$$

Начиная с некоторого n правое неравенство в (5) является строгим.

Если $S \subset Q_n$, то $d_i(S) \leq 1$. Применяя (2), имеем $\xi(S) \geq \alpha(S) \geq n$. С учётом этого (2), (4) и (5) дают

$$\|P\| \geq \frac{2}{n+1} \left(\sum_{i=1}^n \frac{1}{d_i(S)} - 1 \right) + 1, \quad (6)$$

$$\xi_n \geq n, \quad \theta_n \geq 3 - \frac{4}{n+1}. \quad (7)$$

Равенство в (6) достигается тогда и только тогда, когда существует 1-вершина Q_n относительно S и симплекс $\xi(S)S$ описан вокруг Q_n .

Стандартизованным многочленом Лежандра степени n называется функция

$$\chi_n(t) := \frac{1}{2^n n!} [(t^2 - 1)^n]^{(n)}, \quad n = 0, 1, 2, \dots$$

(формула Родрига). Многочлены Лежандра ортогональны на $[-1, 1]$ с весом $w(t) = 1$. Первые многочлены χ_n имеют вид

$$\chi_0(t) = 1, \quad \chi_1(t) = t, \quad \chi_2(t) = \frac{1}{2} (3t^2 - 1), \quad \chi_3(t) = \frac{1}{2} (5t^3 - 3t),$$

$$\chi_4(t) = \frac{1}{8} (35t^4 - 30t^2 + 3), \quad \chi_5(t) = \frac{1}{8} (63t^5 - 70t^3 + 15t).$$

Справедливо рекуррентное соотношение

$$\chi_{n+1}(t) = \frac{2n+1}{n+1}t\chi_n(t) - \frac{n}{n+1}\chi_{n-1}(t).$$

Эти и другие свойства χ_n изложены в [12], [13]. Известно, что $\chi_n(1) = 1$; если $n \geq 1$, то $\chi_n(t)$ возрастает при $t \geq 1$. Обозначим через χ_n^{-1} функцию, обратную к χ_n на полуоси $[1, +\infty)$.

Появление многочленов Лежандра в круге наших вопросов связано с оцениванием θ_n снизу (по поводу подробностей этого метода и доказательств см. [7, гл. 3]). Для $n \in \mathbb{N}$, $\gamma \geq 1$ введём в рассмотрение множество

$$D_{n,\gamma} := \left\{ x \in \mathbb{R}^n : \left| 1 - \sum_{i=1}^n x_i \right| + \sum_{i=1}^n |x_i| \leq \gamma \right\}.$$

В 2003 г. первый автор доказал, что

$$\text{mes}_n(D_{n,\gamma}) = \frac{1}{2^n n!} \sum_{i=0}^n \binom{n}{i}^2 (\gamma - 1)^{n-i} (\gamma + 1)^i = \frac{\chi_n(\gamma)}{n!}. \quad (8)$$

Обозначим через ν_n величину максимального объёма n -мерного симплекса, содержащегося в Q_n . Число ν_n связано со значением h_n максимального 0/1-определителя порядка n равенством $n!\nu_n = h_n$ (см. [19, теорема 2.1]). С применением (8) была доказана оценка

$$\theta_n \geq \chi_n^{-1} \left(\frac{1}{\nu_n} \right). \quad (9)$$

Привлекая известные соотношения для χ_n и ν_n , из (9) удалось получить ряд более обзримых оценок:

$$\begin{aligned} \theta_n &> \frac{\sqrt{n-1}}{e}; \\ \theta_n &> \frac{\sqrt{n}}{e}, \quad n \text{ чётное}; \quad \theta_n > \frac{n}{e\sqrt{n-1}}, \quad n > 1, \quad n \equiv 1 \pmod{4}. \end{aligned}$$

Объединяя результаты (7) и (9), можно записать неравенство

$$\theta_n \geq \max \left[3 - \frac{4}{n+1}, \chi_n^{-1} \left(\frac{1}{\nu_n} \right) \right]. \quad (10)$$

Из других соотношений, систематизированных в [7], отметим следующие. Справедливы двойные оценки

$$n \leq \xi_n < n+1, \quad \frac{1}{4}\sqrt{n} < \theta_n < 3\sqrt{n}.$$

Таким образом, $\xi_n \asymp n$, $\theta_n \asymp \sqrt{n}$. Если S — симплекс максимального объёма в Q_n , P — интерполяционный проектор, узлы которого совпадают с вершинами S , то $\|P\| \asymp \theta_n$, $\xi(S) \asymp \xi_n$. Точными по порядку n оценками сверху для симплекса максимального объёма и соответствующего проектора являются неравенства

$$\xi(S) \leq n+2, \quad \|P\| \leq \min \left(n+1, \frac{4\sqrt{e}}{3}\sqrt{n+2}+1 \right).$$

Число m будем называть *числом Адамара*, если существует матрица Адамара порядка m . По поводу матриц Адамара см., например, [14]. Когда $n + 1$ — число Адамара, и только в этом случае, существует n -мерный правильный симплекс S , для которого $\text{ver}(S) \subset \text{ver}(Q_n)$ (см. [19]). Этот симплекс имеет максимальный объём в Q_n , т. е. для него $\text{vol}(S) = \nu_n$. Выполняется $\xi(S) = n$, откуда $\xi_n = n$ (различные доказательства даются в [7, § 3.2] и [9]). Соответствующий проектор P удовлетворяет неравенству $\|P\| \leq \sqrt{n+1}$ (см. [7, § 3.5]), поэтому в рассматриваемой ситуации $\theta'_n \leq \sqrt{n+1}$.

Главная цель настоящей статьи — публикация новых оценок величины θ_n для конкретных n . К 2009 г. первый автор разными способами установил, что

$$\begin{aligned} \theta_1 = 1, \quad \theta_2 = \frac{2\sqrt{5}}{5} + 1 = 1.89\dots, \quad \theta_3 = 2, \quad 2.2 \leq \theta_4 \leq \frac{7}{3} = 2.33\dots, \\ \frac{7}{3} = 2.33\dots \leq \theta_5 \leq 2.6, \quad \frac{17}{7} = 2.42\dots \leq \theta_6 \leq 3, \quad \theta_7 = 2.5; \\ \xi_1 = 1, \quad \xi_2 = \frac{3\sqrt{5}}{5} + 1 = 2.34\dots, \quad \xi_3 = 3, \quad 4 \leq \xi_4 \leq \frac{13}{3} = 4.33\dots, \\ 5 \leq \xi_5 \leq 5.5, \quad 6 \leq \xi_6 \leq 6.6, \quad \xi_7 = 7. \end{aligned}$$

В дальнейшем некоторые из этих оценок были уточнены. Теоретические результаты общего характера редко дают лучшие верхние оценки для конкретных n . Отмеченные выше свойства делают целесообразным применить для оценивания θ_n и ξ_n сверху симплексы максимального объёма в кубе. Для чисел θ_n , $1 \leq n \leq 20$, такие результаты описаны в [4], см. также [7, § 3.9]. В статье [11] приведены результаты оценивания указанным методом чисел ξ_n для $n \leq 118$. В настоящей статье мы приведём верхние границы чисел θ_n для $21 \leq n \leq 26$, а также лучшие известные оценки этих величин для всех $n \leq 26$.

Для построения симплексов максимального объёма могут применяться 0/1-матрицы порядка n с максимальным определителем. Строки или столбцы такой матрицы, дополненные $(0, \dots, 0)$, дают набор вершин симплекса максимального объёма в Q_n . Максимальный 0/1-определитель порядка n можно получить из максимального $-1/1$ -определителя порядка $n + 1$. Этот подход, впервые применённый в [4], подробно описан в [7, § 3.9] и [11]. Данные о максимальных $-1/1$ -определителях взяты нами с сайта www.indiana.edu/~maxdet.

Мы приведём также лучшие из известных на настоящий момент нижних оценок θ_n для $n \leq 118$.

2. Верхние оценки θ_n

Наиболее точные из полученных авторами оценок θ_n сверху для $1 \leq n \leq 26$ приведены в Таблице 1. В случаях, когда известно точное значение θ_n , приводится это точное значение.

Большая часть оценок получена из рассмотрения проекторов с узлами, расположенными в вершинах симплекса максимального (или предположительно максимального) объёма в Q_n . Для построения таких симплексов при данном n использованы максимальные $-1/1$ -определители порядка $n + 1$.

Таблица 1: Верхние оценки θ_n для $1 \leq n \leq 26$
 Table 1: Upper estimates of θ_n for $1 \leq n \leq 26$

n	min P 	N	$\theta_n \leq$	
1	1	1	$\theta_1 = 1$	АН
2	3	1	$\theta_2 = \frac{2\sqrt{5}}{5} + 1 = 1.8944 \dots$	A
3	2	1	$\theta_3 = 2$	A
4	$\frac{7}{3} = 2.3333 \dots$	1	$\frac{3(4+\sqrt{2})}{7} = 2.3203 \dots$	B
5	$\frac{13}{5} = 2.6$	1	$\frac{13}{5} = 2.6$	AM
6	3	1	2.60014	B
7	$\frac{5}{2} = 2.5$	1	$\theta_7 = \frac{5}{2} = 2.5$	АН
8	$\frac{22}{7} = 3.1428 \dots$	1	$\frac{22}{7} = 3.1428 \dots$	M
9	3	1	3	M
10	$\frac{19}{5} = 3.8$	3	$\frac{19}{5} = 3.8$	M
11	3	1	3	H
12	$\frac{17}{5} = 3.4$	1	$\frac{17}{5} = 3.4$	M
13	$\frac{49}{13} = 3.7692 \dots$	1	$\frac{49}{13} = 3.7692 \dots$	M
14	$\frac{21}{5} = 4.2$	1	$\frac{21}{5} = 4.2$	M
15	$\frac{7}{2} = 3.5$	5	$\frac{7}{2} = 3.5$	H
16	$\frac{21}{5} = 4.2$	3	$\frac{21}{5} = 4.2$	M
17	$\frac{139}{34} = 4.0882 \dots$	3	$\frac{139}{34} = 4.0882 \dots$	M
18	$\frac{95}{17} = 5.5882 \dots$	3	$\frac{95}{17} = 5.5882 \dots$	M
19	4	3	4	H
20	$\frac{137}{29} = 4.7241 \dots$	7	$\frac{137}{29} = 4.7241 \dots$	M
21	$\frac{251}{50} = 5.02$	1	$\frac{251}{50} = 5.02$	M?
22	$\frac{1817}{335} = 5.4238 \dots$	1	$\frac{1817}{335} = 5.4238 \dots$	M?
23	$\frac{9}{2} = 4.5$	60	$\frac{9}{2} = 4.5$	BH
24	$\frac{103}{21} = 4.9047 \dots$	2	$\frac{103}{21} = 4.9047 \dots$	M
25	5	3	5	M
26	$\frac{474}{91} = 5.2087 \dots$	1	$\frac{474}{91} = 5.2087 \dots$	M?

Максимальность $-1/1$ -определителей порядка $1, \dots, 21$, приведённых на сайте www.indiana.edu/~maxdet, доказана. Более того, на сайте приведены все (с точностью до эквивалентности матриц) максимальные определители порядка ≤ 21 . При получении оценок нами были использованы все эти данные. Максимальность определителей порядков 22, 23 и 27 не установлена. Такие ситуации отмечены в таблице знаком вопроса. Неясно, является ли исчерпывающим приведённый на сайте набор максимальных определителей порядков 25 и 26. Для уточнения верхней оценки θ_n рассматривались все известные нам максимальные $-1/1$ -определители порядка $n + 1$, так как соответствующие проекторы могут иметь различную норму.

Во всех ситуациях, когда $n + 1$ есть число Адамара, нами использован полный набор адамаровых матриц соответствующего порядка. В частности, для получения оценки θ_{23} были рассмотрены все существующие 60 матриц Адамара порядка 24. Этот трудоёмкий случай был отдельно изучен А. Ю. Ухаловым и Е. А. Озеровой (см. [2]).

Вычисления по формуле (3) требуют перебора всех 2^n вершин Q_n . При больших n вычисления становятся довольно трудоёмкими. По этой причине мы ограничились исследованием случаев $1 \leq n \leq 26$. Для оценивания θ_{27} пришлось бы рассмотреть 487 матриц Адамара порядка 28. Получение этой оценки требует привлечения мощных вычислительных средств.

Если $n + 1$ — число Адамара, то каждый из симплексов максимального объема в Q_n является правильным и его вершины совпадают с вершинами куба. Может показаться, что все эти симплексы расположены в кубе одинаково и достаточно рассмотреть один из них. Наши вычисления, однако, показывают, что это не так. Узлы интерполяционных проекторов, соответствующие различным правильным симплексам, могут располагаться внутри куба различным образом. Эти проекторы могут иметь разные нормы.

Из рассматриваемых нами адамаровых $n + 1$ в четырёх случаях, а именно для порядков 2, 4, 8, 12, существует всего одна (с точностью до эквивалентности) матрица Адамара. Для каждого из остальных адамаровых $n + 1$ эта матрица не является единственной. Опишем эти случаи отдельно.

Имеется пять попарно неэквивалентных матриц Адамара порядка 16. Для соответствующих пяти проекторов $\|P_1\| = \|P_2\| = \|P_3\| = 4$, $\|P_4\| = \|P_5\| = \frac{7}{2}$. Отсюда следует, что 15-мерный правильный симплекс может быть вписан в куб Q_{15} принципиально по-разному. Более точно, существуют вписанные в Q_{15} правильные симплексы S^* , S^{**} , такие что S^* не переводится в S^{**} с помощью ортогонального преобразования, отображающего куб в себя.

Различное расположение правильных симплексов внутри куба возможно даже в случае, когда нормы соответствующих проекторов совпадают. Такая ситуация может быть выявлена с помощью подсчёта количества μ -вершин для соответствующего проектора (см. п. 1). Распределение μ -вершин для проекторов $P_1, \dots, P_5$ приведено в Таблице 2. Несмотря на то, что нормы P_1 , P_2 и P_3 совпадают, количество 6-вершин для них различается. Это говорит о различном расположении соответствующих симплексов в Q_{15} .

Существует три неэквивалентные матрицы Адамара порядка 20, однако для всех трёх полученных из этих матриц проекторов норма одинакова и равна 4. Отсюда следует, что $\theta_{19} \leq 4$.

Таблица 2: Количество μ -вершин для проекторов P_i
 Table 2: Number of μ -vertices for projectors P_i

$i \backslash \mu$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	0	0	0	0	0	448	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	192	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	64	0	0	0	0	0	0	0	0	0
4	0	0	0	896	1344	5376	0	1344	0	0	0	0	0	0	0
5	0	0	0	896	1344	5376	0	1344	0	0	0	0	0	0	0

Для следующего адамарова числа 24 имеется уже 60 попарно неэквивалентных матриц Адамара. В этом случае также существуют различные значения норм проектора. Для четырёх матриц норма проектора оказалась равной $\frac{9}{2} = 4.5$, а для всех остальных матриц это значение равно $\frac{14}{3} = 4.6666 \dots$. Следовательно, $\theta_{23} \leq \frac{9}{2}$. Распределение μ -вершин для этого случая еще более разнообразно, чем в случае $n = 15$. Различным значениям нормы и наборам μ -вершин соответствуют различные расположения правильного симплекса внутри куба Q_{23} .

Нормы могут различаться и в случаях, когда число $n + 1$ не является адамаровым. Например, для получения оценки θ_{25} нами были рассмотрены три $-1/1$ -матрицы порядка 26 с максимальным определителем. Построенные на их основе проекторы T_1 , T_2 и T_3 имеют нормы $\|T_1\| = \|T_2\| = \frac{127}{25} = 5.08$, $\|T_3\| = 5$.

Для случаев $n = 4$ и $n = 6$ оценки θ_n , следующие из рассмотрения максимальных определителей, удалось улучшить. Эти результаты были получены А. Ю. Ухаловым и И. С. Кудрявцевым с помощью численной минимизации нормы проектора (см. [2]).

Оценка θ_4 получается из рассмотрения проектора P' по узлам

$$\left(1, 1 - \frac{1}{\sqrt{2}}, 0, 0\right), \quad \left(1, 1, \frac{1}{\sqrt{2}}, 1\right), \quad \left(\frac{1}{2}, 0, 1, \frac{1}{2}\right), \quad \left(0, 1 - \frac{1}{\sqrt{2}}, 0, 1\right), \quad \left(0, 1, \frac{1}{\sqrt{2}}, 0\right).$$

Для этого проектора по формуле (3) находим $\|P'\| = \frac{3(4+\sqrt{2})}{7} = 2.320377 \dots$. При численной минимизации координаты узлов P' были получены в виде десятичных дробей. Значения, содержащие квадратные корни, были найдены с помощью функции распознавания чисел сайта Wolfram Alpha (<http://www.wolframalpha.com>). После замены дробей распознанными величинами значение нормы уменьшилось. Итак, $\theta_4 \leq \frac{3(4+\sqrt{2})}{7} = 2.320377 \dots$.

Верхняя граница θ_6 получается из рассмотрения проектора P'' с узлами

$$\begin{aligned} &(1, 0, 1, 0.091, 0, 0.4999), \quad (0, 1, 1, 1, 0, 0), \quad (0.5, 1, 1, 0.091, 1, 1), \\ &(0.9106, 0.0896, 0.0895, 1, 0.91053, 0.9106), \quad (0, 0, 0.5, 0.09115, 1, 0), \\ &(0, 0.49999, 0, 0.09104, 0, 1), \quad (1, 1, 0, 0.09105, 0.5001, 0). \end{aligned}$$

С помощью (3) находим $\|P''\| = 2.600137227 \dots$. Значит, $\theta_6 < 2.60014$.

Справедливы двойные неравенства

$$\frac{11}{5} = 2.2 \leq \theta_4 \leq \frac{3(4 + \sqrt{2})}{7} = 2.320377 \dots, \quad (11)$$

$$\frac{17}{7} = 2.42857 \dots \leq \theta_6 < 2.60014. \quad (12)$$

Оценки снизу в (11) и (12) получаются из (7). Отметим, что разница между верхней и нижней границами в неравенстве (11) не превосходит 0.13, а в неравенстве (12) не превосходит 0.18. Таким образом, величины θ_4 и θ_6 оценены с довольно высокой точностью.

Авторы настоящей работы предполагают, что P' является минимальным проектором, т. е. $\theta_4 = \frac{3(4+\sqrt{2})}{7} = 2.320377 \dots$

В первом столбце Таблицы 1 даётся размерность пространства n . Второй столбец содержит минимальную норму проектора, полученную из рассмотрения максимальных $-1/1$ -определителей порядка $n + 1$. В третьем столбце таблицы приводится количество N матриц порядка $n + 1$, рассмотренных для получения результата второго столбца. В четвёртом столбце даётся лучшая известная верхняя оценка θ_n для данного n . Последний столбец таблицы содержит комментарий о способе получения верхней границы θ_n , указанной в четвёртом столбце. При этом используются следующие обозначения.

- А — точное значение θ_n получено ранее первым автором, см. [7].
- В — оценка сверху получена в работе [2].
- М — использован симплекс максимального объема в Q_n , построенный из максимального $-1/1$ -определителя порядка $n + 1$.
- М? — использован симплекс, построенный из наибольшего известного определителя порядка $n + 1$. Максимальность данного определителя не доказана.
- Н — число $n + 1$ является адамаровым. Использован правильный симплекс, построенный из соответствующей матрицы Адамара.

Отметим, что числа, стоящие во втором столбце Таблицы 1, при всех n являются верхними границами величины θ'_n .

Для вычислений и подготовки таблиц использовался набор программ на языке Wolfram Language (см., например, [21]).

3. Нижние оценки θ_n

В Таблицах 3, 4, 5 представлены лучшие из известных нижних оценок θ_n . Для получения этих оценок использовалось неравенство (10). Для каждого n приводятся значения функций $\chi_n^{-1}(\frac{1}{\nu_n})$ и $3 - \frac{4}{n+1}$, а также максимальное из них. Этот максимум и является наиболее точной нижней границей θ_n . В таблицах отсутствуют значения для $n = 104$ и $n = 116$, так как на сайте www.indiana.edu/~maxdet не приведены максимальные определители порядков 105 и 117.

Таблица 3: Нижние оценки θ_n для $1 \leq n \leq 54$
 Table 3: Lower estimates of θ_n for $1 \leq n \leq 54$

n	$\chi_n^{-1}(\frac{1}{\nu_n})$	$3 - \frac{4}{n+1}$	Max	n	$\chi_n^{-1}(\frac{1}{\nu_n})$	$3 - \frac{4}{n+1}$	Max
1	1	1	1	28	2.2768	2.8621	2.8621
2	1.291	1.6667	1.6667	29	2.3074	2.8667	2.8667
3	1.2492	2	2	30	2.3487	2.871	2.871
4	1.3478	2.2	2.2	31	2.3452	2.875	2.875
5	1.4284	2.3333	2.3333	32	2.3955	2.8788	2.8788
6	1.5018	2.4286	2.4286	33	2.4259	2.8824	2.8824
7	1.4678	2.5	2.5	34	2.4642	2.8857	2.8857
8	1.5626	2.5556	2.5556	35	2.4601	2.8889	2.8889
9	1.6034	2.6	2.6	36	2.5019	2.8919	2.8919
10	1.6699	2.6364	2.6364	37	2.5348	2.8947	2.8947
11	1.6488	2.6667	2.6667	38	2.5722	2.8974	2.8974
12	1.7086	2.6923	2.6923	39	2.5697	2.9	2.9
13	1.7659	2.7143	2.7143	40	2.6056	2.9024	2.9024
14	1.8211	2.7333	2.7333	41	2.641	2.9048	2.9048
15	1.8108	2.75	2.75	42	2.6759	2.907	2.907
16	1.8778	2.7647	2.7647	43	2.6747	2.9091	2.9091
17	1.9156	2.7778	2.7778	44	2.7179	2.9111	2.9111
18	1.965	2.7895	2.7895	45	2.743	2.913	2.913
19	1.9587	2.8	2.8	46	2.7791	2.9149	2.9149
20	2.0159	2.8095	2.8095	47	2.7756	2.9167	2.9167
21	2.0588	2.8182	2.8182	48	2.8201	2.9184	2.9184
22	2.1039	2.8261	2.8261	49	2.8413	2.92	2.92
23	2.0958	2.8333	2.8333	50	2.8805	2.9216	2.9216
24	2.1408	2.84	2.84	51	2.8729	2.9231	2.9231
25	2.1847	2.8462	2.8462	52	2.9173	2.9245	2.9245
26	2.2278	2.8519	2.8519	53	2.9362	2.9259	2.9362
27	2.2242	2.8571	2.8571	54	2.9735	2.9273	2.9735

Таблица 4: Нижние оценки θ_n для $55 \leq n \leq 109$
Table 4: Lower estimates of θ_n for $55 \leq n \leq 109$

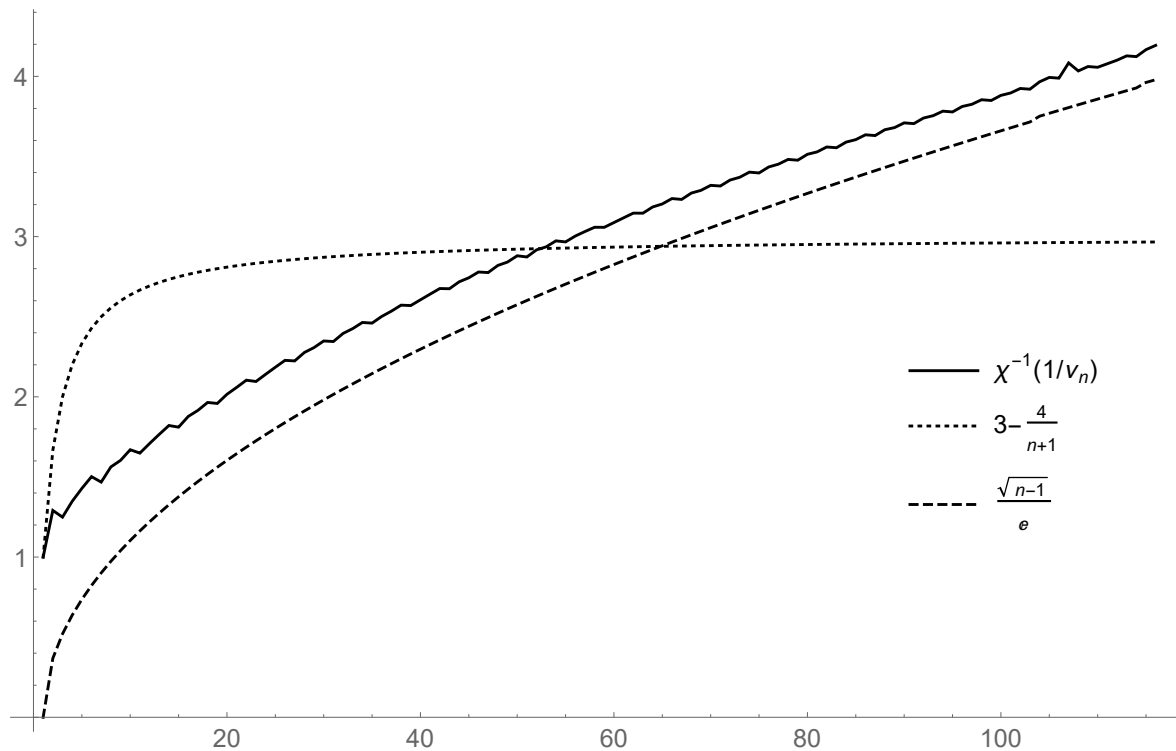
n	$\chi_n^{-1}(\frac{1}{\nu_n})$	$3 - \frac{4}{n+1}$	Max	n	$\chi_n^{-1}(\frac{1}{\nu_n})$	$3 - \frac{4}{n+1}$	Max
55	2.9669	2.9286	2.9669	82	3.5595	2.9518	3.5595
56	3.0034	2.9298	3.0034	83	3.5546	2.9524	3.5546
57	3.0315	2.931	3.0315	84	3.5899	2.9529	3.5899
58	3.0583	2.9322	3.0583	85	3.6053	2.9535	3.6053
59	3.058	2.9333	3.058	86	3.6355	2.954	3.6355
60	3.0877	2.9344	3.0877	87	3.6307	2.9545	3.6307
61	3.1173	2.9355	3.1173	88	3.667	2.9551	3.667
62	3.1465	2.9365	3.1465	89	3.6803	2.9556	3.6803
63	3.1463	2.9375	3.1463	90	3.7099	2.956	3.7099
64	3.1849	2.9385	3.1849	91	3.7052	2.9565	3.7052
65	3.2039	2.9394	3.2039	92	3.7401	2.957	3.7401
66	3.2375	2.9403	3.2375	93	3.755	2.9574	3.755
67	3.2322	2.9412	3.2322	94	3.783	2.9579	3.783
68	3.2717	2.942	3.2717	95	3.7781	2.9583	3.7781
69	3.2888	2.9429	3.2888	96	3.8121	2.9588	3.8121
70	3.32	2.9437	3.32	97	3.8258	2.9592	3.8258
71	3.3158	2.9444	3.3158	98	3.8542	2.9596	3.8542
72	3.3529	2.9452	3.3529	99	3.8497	2.96	3.8497
73	3.3703	2.9459	3.3703	100	3.8814	2.9604	3.8814
74	3.4023	2.9467	3.4023	101	3.8964	2.9608	3.8964
75	3.3973	2.9474	3.3973	102	3.9246	2.9612	3.9246
76	3.4348	2.9481	3.4348	103	3.92	2.9615	3.92
77	3.4521	2.9487	3.4521	105	3.9662	2.9623	3.9662
78	3.4818	2.9494	3.4818	106	3.9936	2.9626	3.9936
79	3.4769	2.95	3.4769	107	3.989	2.963	3.989
80	3.5138	2.9506	3.5138	108	4.0841	2.9633	4.0841
81	3.5288	2.9512	3.5288	109	4.034	2.9636	4.034

Таблица 5: Нижние оценки θ_n для $110 \leq n \leq 118$
 Table 5: Lower estimates of θ_n for $110 \leq n \leq 118$

n	$\chi_n^{-1}(\frac{1}{\nu_n})$	$3 - \frac{4}{n+1}$	Max	n	$\chi_n^{-1}(\frac{1}{\nu_n})$	$3 - \frac{4}{n+1}$	Max
110	4.0615	2.964	4.0615	114	4.1281	2.9652	4.1281
111	4.0568	2.9643	4.0568	115	4.1234	2.9655	4.1234
112	4.0789	2.9646	4.0789	117	4.167	2.9661	4.167
113	4.101	2.9649	4.101	118	4.1937	2.9664	4.1937

Результаты вычислений даются с точностью до 10^{-4} .

Графики функций $\chi_n^{-1}(\frac{1}{\nu_n})$, $3 - \frac{4}{n+1}$ и $\frac{\sqrt{n-1}}{e}$ приведены на Рис. 1. Эти функции определены лишь для целочисленных значений аргумента. Однако для удобства восприятия при построении графиков использовались непрерывные линии различных типов. Неравенство $\chi_n^{-1}(\frac{1}{\nu_n}) > 3 - \frac{4}{n+1}$ выполняется при $n \geq 53$ (см. Таблицу 3).


 Рис. 1: Графики функций $\chi_n^{-1}(\frac{1}{\nu_n})$, $3 - \frac{4}{n+1}$ и $\frac{\sqrt{n-1}}{e}$
 Fig. 1: Graphs of the functions $\chi_n^{-1}(\frac{1}{\nu_n})$, $3 - \frac{4}{n+1}$, and $\frac{\sqrt{n-1}}{e}$

4. О выполнении неравенства $\xi_n < \frac{n+1}{2}(\theta_n - 1) + 1$

Как отмечалось в п. 1, при любом n справедливо неравенство

$$\xi_n \leq \frac{n+1}{2}(\theta_n - 1) + 1. \quad (13)$$

На настоящий момент мы знаем лишь четыре значения n , при которых в этом соотношении имеет место равенство: $n = 1, 2, 3$ и 7 . Это ровно те случаи, в которых известны точные значения θ_n и ξ_n . В [8] авторы выдвинули предположение, что минимальное n , при котором неравенство в (13) является строгим, равно 4.

Заметим, что точное значение $\xi_n = n$ известно для всех n , когда $n+1$ есть число Адамара, а также для $n = 5$ и $n = 9$. Во всех этих случаях (13) эквивалентно $\theta_n \geq 3 - \frac{4}{n+1}$, а равенство в (13) равносильно $\theta_n = 3 - \frac{4}{n+1}$. Такое точное значение θ_n достигается лишь в ситуации, когда для некоторого симплекса S с условием $\xi(S) = \xi_n$ существует 1-вершина Q_n относительно S (см. п. 1). Однако наши вычисления показывают, что для всех отмеченных $n \leq 24$, когда $\xi_n = n$, 1-вершины куба относительно симплекса, экстремального в смысле ξ_n , существуют только для $n = 1, 2, 3, 7$.

Из асимптотических соотношений $\xi_n \asymp n$, $\theta_n \asymp \sqrt{n}$ следует, что для всех достаточно больших n справедливо строгое неравенство

$$\xi_n < \frac{n+1}{2}(\theta_n - 1) + 1. \quad (14)$$

Обозначим через n_0 минимальное натуральное число, такое что при $n \geq n_0$ верно (14). Вопрос о точном значении n_0 является очень трудным. Известные нижняя и верхняя границы различаются весьма существенно. Из предыдущего имеем оценку снизу $n_0 \geq 8$. Применяя (9) и асимптотические свойства многочленов Лежандра, первый автор в 2009 г. доказал, что $n_0 \leq 57$ (см. [5], [7, § 3.7]). Достаточным условием для выполнения (14) при $n > 2$ является неравенство

$$\chi_n \left(\frac{3n-5}{n-1} \right) \cdot \nu_n < 1. \quad (15)$$

Наши последние вычисления позволяют несколько понизить верхнюю границу числа n_0 . Опишем соответствующие результаты.

Первый подход использует собранные в [11] верхние границы чисел ξ_n и приведённые в п. 3 нижние границы чисел θ_n . Обозначим эти границы через a_n и b_n соответственно. Положим $c_n := \frac{n+1}{2}(b_n - 1) + 1$. Нас интересует то значение n , начиная с которого $a_n < c_n$. Располагая оценками для $n \leq 118$, мы обнаружили, что указанное соотношение для a_n и c_n выполняется начиная с $n = 53$. Данные для $41 \leq n \leq 60$ приводятся в Таблице 6.

Второй подход базируется на условии (15), гарантирующем строгое неравенство (14). Вычисления показывают, что (15), а с ним и (14), выполняются при $n \geq 54$. Поведение величины $\chi_n \left(\frac{3n-5}{n-1} \right) \cdot \nu_n$ представлено на Рис. 2 и Рис. 3.

Таким образом, $n_0 \leq 53$. Иначе говоря, строгое неравенство (14) выполняется по крайней мере начиная с $n = 53$.

Таблица 6: Числа a_n и c_n для $41 \leq n \leq 60$
 Table 6: Numbers a_n and c_n for $41 \leq n \leq 60$

n	a_n	c_n	$a_n - c_n$	n	a_n	c_n	$a_n - c_n$
41	41.361	35.4612	5.89973	51	51	49.6955	1.30445
42	42.5439	37.0328	5.51107	52	52.9608	51.8073	1.15348
43	43	37.8441	5.15592	53	53.2758	53.2783	-0.00258699
44	44.9535	39.6528	5.30067	54	54.5135	55.2709	-0.757386
45	45.3273	41.0896	4.23764	55	55	56.0734	-1.07339
46	46.9556	42.8086	4.14692	56	56.2857	58.0955	-1.80977
47	47	43.6153	3.38472	57	57.6179	59.9143	-2.29645
48	48.9574	45.5916	3.3659	58	58.3581	61.7212	-3.3631
49	49.2143	47.0327	2.18158	59	59	62.7385	-3.7385
50	50.5217	48.9515	1.57023	60	60.1515	64.6762	-4.52468

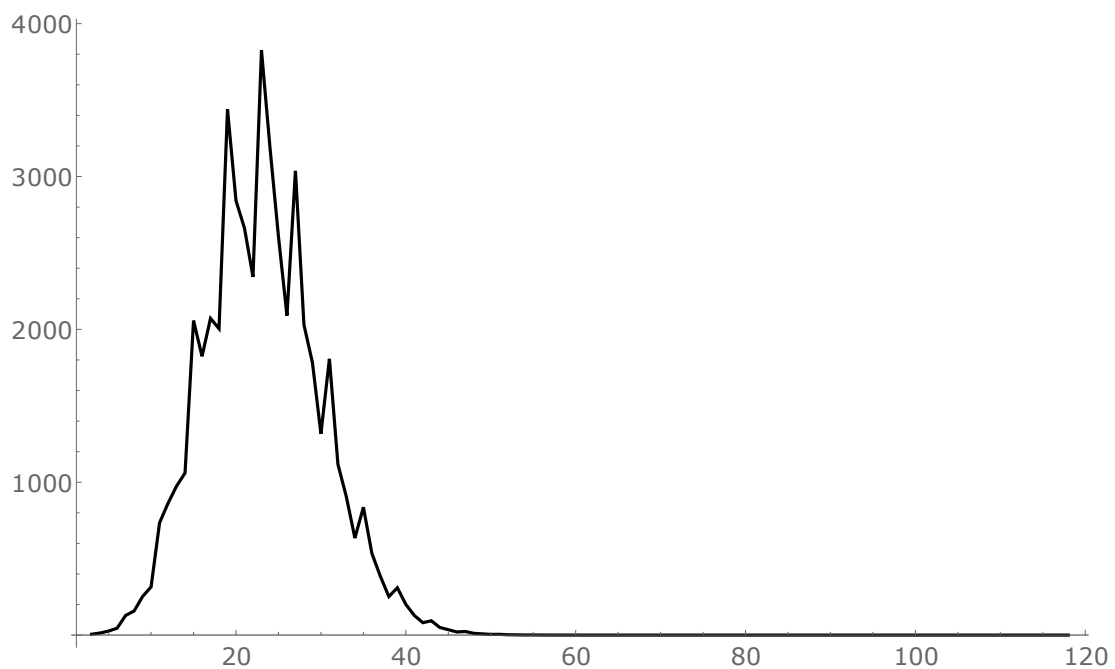


Рис. 2: График функции $\chi_n \left(\frac{3n-5}{n-1} \right) \cdot \nu_n$ для $n \geq 3$
 Fig. 2: Graph of the function $\chi_n \left(\frac{3n-5}{n-1} \right) \cdot \nu_n$ for $n \geq 3$

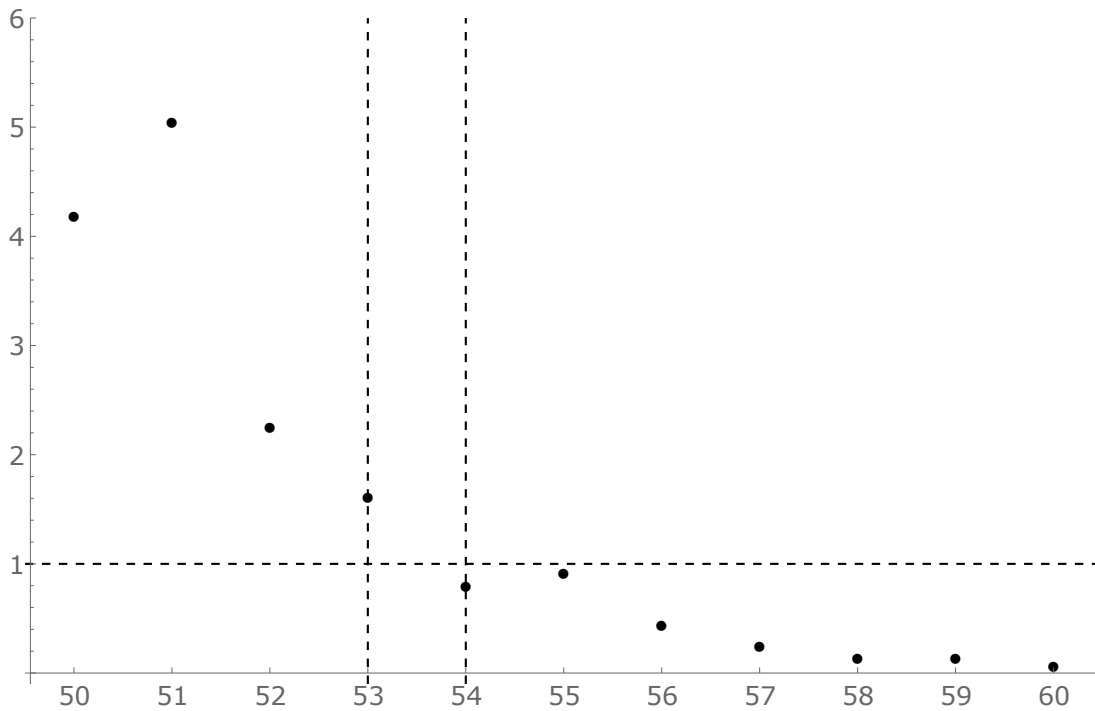


Рис. 3: Величина $\chi_n \left(\frac{3n-5}{n-1} \right) \cdot \nu_n$ для $50 \leq n \leq 60$

Fig. 3: Value $\chi_n \left(\frac{3n-5}{n-1} \right) \cdot \nu_n$ for $50 \leq n \leq 60$

5. О равноотсечении для правильного симплекса, вписанного в куб

Как мы отметили выше, в случае, когда число $n + 1$ является адамаровым, правильные симплексы, вписанные в Q_n , могут быть расположены относительно вершин куба по-разному. В частности, это ведёт к тому, что нормы интерполяционных проекторов, соответствующих различным симплексам, могут различаться. Однако каждый правильный симплекс S , вписанный в куб, обладает следующим *свойством равноотсечения*. Каждая из $n + 1$ частей, отсекаемых от куба (во внешнюю относительно симплекса сторону) гиперплоскостями $(n - 1)$ -мерных граней S имеет один и тот же объём. Величина этого объёма σ_n зависит только от n , а не от симплекса S . Это свойство правильных симплексов отмечалось авторами в [10], где было сказано, что оно следует из симметрии S . В настоящем пункте мы дадим подробное обоснование этого свойства, а также приведём явные формулы для σ_n и асимптотику этой величины при $n \rightarrow \infty$.

Вопросы, связанные с равноотсечением симплексов, рассматривались также в работе [1], где были описаны некоторые семейства двумерных и трёхмерных симплексов с таким свойством.

Пусть k — натуральное, $k \leq n$. *Эйлеровым числом* $A_{n,k}$ называется количество перестановок порядка n , каждая из которых имеет ровно $k - 1$ снижений, т. е. инверсий соседних компонент. Это определение даётся в [18, § 6.2] и [17]. К введению чисел $A_{n,k}$ имеются и другие подходы (см., например, [7, гл. 4]).

Введём в рассмотрение слои куба Q_n , получающиеся при его пересечении гипер-

плоскостями, ортогональными главной диагонали:

$$T_{n,k} := \left\{ x \in Q_n : k-1 \leq \sum_{i=1}^n x_i \leq k \right\}, \quad k = 1, \dots, n.$$

Имеют место равенства

$$A_{n,k} = \sum_{j=0}^{k-1} (-1)^j \binom{n+1}{j} (k-j)^n, \quad (16)$$

$$\text{vol}(T_{n,k}) = \frac{A_{n,k}}{n!}, \quad (17)$$

$$\sum_{k=1}^n A_{n,k} = n!, \quad (18)$$

$$A_{n,k} = (n-k+1)A_{n-1,k-1} + kA_{n-1,k}. \quad (19)$$

Равенство (16) получено в [16]. Соотношение (17) найдено Лапласом [20]; короткое доказательство принадлежит Стенли [26]. Геометрические построения, ведущие к (17), рассматривались Зоммерфельдом (см. обзор [15]). Так как $\sum \text{vol}(T_{n,k}) = \text{vol}(Q_n) = 1$, то из (17) получается (18). Конечно, (18) следует и из того, что число всех перестановок порядка n равно $n!$. При вычислении эйлеровых чисел по рекуррентному соотношению (19) для $k < 1$ и для $k > n$ надо взять $A_{n,k} = 0$. Первые эйлеровы числа приведены в Таблице 7. Числа $A_{n,k}$ быстро растут с ростом n . Например, $A_{15,8} = 447\,538\,817\,472$, а $A_{20,10} = 679\,562\,217\,794\,156\,938$.

Таблица 7: Эйлеровы числа для $1 \leq n \leq 10$
Table 7: Eulerian numbers for $1 \leq n \leq 10$

$n \backslash k$	1	2	3	4	5	6	7	8	9	10
1	1									
2	1	1								
3	1	4	1							
4	1	11	11	1						
5	1	26	66	26	1					
6	1	57	302	302	57	1				
7	1	120	1191	2416	1191	120	1			
8	1	247	4293	15619	15619	4293	247	1		
9	1	502	14608	88234	156190	88234	14608	502	1	
10	1	1013	47840	455192	1310354	1310354	455192	47840	1013	1

Пусть $u \in \mathbb{R}$. Обозначим

$$G_{n,u} := \left\{ x \in Q_n : \sum_{i=1}^n x_i = u \right\}, \quad s(n, u) := \text{mes}_{n-1}(G_{n,u}).$$

Для $j = 1, \dots, n-1$ верно $s(n, j) = \frac{\sqrt{n}}{(n-1)!} \cdot A_{n-1, j}$. Доказательство этого и других соотношений для эйлеровых чисел дано в [3] (см. также [7, гл. 4]).

Центральным B -сплайном порядка n называется функция

$$B_n(t) := \frac{2}{\pi} \int_0^\infty \left(\frac{\sin \xi}{\xi} \right)^n \cos(2t\xi) d\xi.$$

Это чётная кусочно-полиномиальная функция степени $n-1$, принадлежащая $C^{n-2}(\mathbb{R})$. Носитель B_n есть $(-\frac{n}{2}, \frac{n}{2})$; если $|t| < n/2$, то $B_n(t) > 0$. Кроме того,

$$\int_{-\infty}^{\infty} B_n(t) dt = 1.$$

Для вычислений с B -сплайнами могут применяться формулы

$$B_n(t) = \frac{1}{(n-1)!} \sum_{k=0}^n (-1)^k \binom{n}{k} \left(t + \frac{n}{2} - k \right)_+^{n-1},$$

$$B_n(t) = \frac{1}{(n-1)!} \sum_{k=0}^{[n/2-|t|]} (-1)^k \binom{n}{k} \left(\frac{n}{2} - |t| - k \right)^{n-1}, \quad |t| \leq \frac{n}{2}.$$

Здесь

$$a_+^m := \begin{cases} a^m, & a \geq 0, \\ 0, & a < 0, \end{cases} \quad \text{если } a \text{ или } m \neq 0; \quad 0_+^0 := \frac{1}{2}.$$

Свойства и история B -сплайнов приведены, например, в [15]. Первым, кто выявил связь B -сплайнов с сечениями n -мерного куба, был Зоммерфельд [25]. Им доказаны важные соотношения

$$B_n(t) = \frac{1}{\sqrt{n}} s\left(n, t + \frac{n}{2}\right), \quad n > 1; \quad B_n(t) \cong \sqrt{\frac{6}{\pi n}} \cdot e^{-6t^2/n}.$$

Из этих соотношений, в частности, получаются следующие результаты об асимптотике мер центрального сечения $G_{n, \frac{n}{2}}$ и близкого к нему сечения $G_{n, \frac{n+1}{2}}$:

$$\text{mes}_{n-1}(G_{n, \frac{n}{2}}) = s\left(n, \frac{n}{2}\right) = \sqrt{n} \cdot B_n(0) \cong \sqrt{\frac{6}{\pi}},$$

$$\text{mes}_{n-1}\left(G_{n, \frac{n+1}{2}}\right) = s\left(n, \frac{n+1}{2}\right) = \sqrt{n} \cdot B_n\left(\frac{1}{2}\right) \cong \sqrt{\frac{6}{\pi}} \cdot e^{-3/(2n)}.$$

Таким образом,

$$\lim_{n \rightarrow \infty} \text{mes}_{n-1}(G_{n, \frac{n}{2}}) = \lim_{n \rightarrow \infty} \text{mes}_{n-1}\left(G_{n, \frac{n+1}{2}}\right) = \sqrt{\frac{6}{\pi}}. \quad (20)$$

Теорема 1. Пусть $n+1$ — число Адамара, большее 2, S — произвольный n -мерный правильный симплекс, вершины которого совпадают с вершинами Q_n . Обозначим через $D_1, \dots, D_{n+1}$ внешние по отношению к S части куба, отсекаемые от Q_n гиперплоскостями $(n-1)$ -мерных граней S . Тогда

$$\begin{aligned} \text{vol}(D_1) &= \dots = \text{vol}(D_{n+1}) = \\ &= \frac{1}{n!} \sum_{k=\frac{n+1}{2}+1}^n A_{n,k} = \frac{1}{n!} \sum_{k=\frac{n+1}{2}+1}^n \sum_{j=0}^{k-1} (-1)^j \binom{n+1}{j} (k-j)^n. \end{aligned} \quad (21)$$

Доказательство. Сначала напомним, что длина любого ребра симплекса S равна $\sqrt{\frac{n+1}{2}}$. Действительно, так как число $n+1$ — адамарово, то существует матрица Адамара $\mathbf{H}$ порядка $n+1$. Элементы этой матрицы равны 1 или -1 , а строки и столбцы попарно ортогональны. Система строк и система столбцов задают наборы вершин двух правильных симплексов, вписанных в куб $[-1, 1]^n$. Рассмотрим правильный симплекс S' , построенный на строках $\mathbf{H}$ как на вершинах. В силу попарной ортогональности строк для любых двух вершин S'

$$\|a - b\|^2 = (a - b, a - b) = \|a\|^2 + \|b\|^2 = 2(n+1)$$

(так как координаты вершин суть ± 1). Значит, длина любого ребра S' равна $\sqrt{2(n+1)}$. Из соображений подобия следует, что длина ребра правильного симплекса S , вписанного в $Q_n = [0, 1]^n$, в 2 раза меньше, т. е. составляет $\sqrt{\frac{n+1}{2}}$.

Пусть D — любая из частей D_k из условия теоремы. Обозначим через v ту единственную вершину S , которая не принадлежит D . Без ограничения общности можно считать, что $v = 0$. (Если это не так, выберем в $\mathbb{R}^n$ новую систему координат, начало которой совпадает с v , а оси координат задаются рёбрами куба, исходящими из этой точки.) Поскольку длина ребра S равна $\sqrt{\frac{n+1}{2}}$, а координаты вершин S равны 0 и 1, то все вершины симплекса, отличные от v , принадлежат гиперплоскости $\sum x_i = \frac{n+1}{2}$. Следовательно,

$$D = \left\{ x \in Q_n : \sum_{i=1}^n x_i \geq \frac{n+1}{2} \right\} = \bigcup_{k=\frac{n+1}{2}+1}^n T_{n,k}.$$

Таким образом,

$$\text{vol}(D) = \sum_{k=\frac{n+1}{2}+1}^n T_{n,k}.$$

Остаётся применить формулы (17) и (16). Теорема доказана. $\square$

Заметим, что свойство равноотсечения тривиальным образом выполняется и в случае $n = 1$, когда $S = Q_1 = [0, 1]$ и $\text{vol}(D_1) = \text{vol}(D_2) = 0$.

Обозначим величину, стоящую в (21), через σ_n . Пусть

$$E := \left\{ x \in Q_n : \frac{n}{2} \leq \sum_{i=1}^n x_i \leq \frac{n+1}{2} \right\}, \quad R := \left\{ x \in Q_n : \sum_{i=1}^n x_i \geq \frac{n}{2} \right\}.$$

Ясно, что $\text{vol}(R) = \frac{1}{2}$. Высота слоя E в направлении большой диагонали куба равна $\frac{1}{2\sqrt{n}}$. Значит, объём E не превосходит $\frac{m}{2\sqrt{n}}$, где m — максимальная из $(n-1)$ -мер сечений $G_{n, \frac{n}{2}}$ и $G_{n, \frac{n+1}{2}}$. Применяя (20), получаем, что с ростом размерности $\text{vol}(E)$ стремится к нулю. Тем самым,

$$\sigma_n = \text{vol}(R) - \text{vol}(E) \rightarrow \frac{1}{2}, \quad n \rightarrow \infty.$$

Соотношение

$$0 \leq \text{vol}(E) = \frac{1}{2} - \sigma_n \leq \frac{m}{2\sqrt{n}}$$

означает, что $\frac{1}{2} - \sigma_n = O(n^{-1/2})$. Так как $m \rightarrow \sqrt{\frac{6}{\pi}}$, см. (20), то оценка

$$\frac{1}{2} - \sigma_n \leq C \cdot n^{-1/2}, \quad n+1 - \text{адамарово}, \quad n > n_1,$$

за счёт выбора n_1 гарантируется с любой константой $C > \sqrt{\frac{3}{2\pi}} = 0.690988\dots$. Например, при всех достаточно больших n , таких что $n+1$ есть число Адамара, выполняется неравенство $\frac{1}{2} - \sigma_n \leq 0.7n^{-1/2}$.

Список литературы / References

- [1] Есипова Е. М., “Геометрические характеристики симплексов, обладающих свойством равноотсечения”, *Современные проблемы математики и информатики*, **17**, Ярославский государственный университет им. П. Г. Демидова, Ярославль, 2017, 49–61; [Esipova E. M., “Geometricheskie haracteristiki simpleksov, obladayuschih svoistvom ravnootsecheniya”, *Sovremennye problemy matematiki i informatiki*, **17**, P. G. Demidov Yaroslavl State University, Yaroslavl, 2017, 49–61, (in Russian).]
- [2] Кудрявцев И. С., Озерова Е. А., Ухалов А. Ю., “Новые оценки для норм минимальных проекторов”, *Современные проблемы математики и информатики*, **17**, Ярославский государственный университет им. П. Г. Демидова, Ярославль, 2017, 74–81; [Kudryavtsev I. S., Ozerova E. A., Ukhlov A. Yu., “Novye ocenki dlya norm minimalnyh proektorov”, *Sovremennye problemy matematiki i informatiki*, **17**, P. G. Demidov Yaroslavl State University, Yaroslavl, 2017, 74–81, (in Russian).]
- [3] Невский М. В., “Ортогональное проектирование и минимальная линейная интерполяция на n -мерном кубе”, *Модел. и анализ информ. систем*, **14:3** (2007), 8–28; [Nevskij M. V., “Orthogonal projection and minimal linear interpolation on an n -dimensional cube”, *Modeling and Analysis of Information Systems*, **14:3** (2007), 8–28, (in Russian).]
- [4] Невский М. В., Хлесткова И. В., “К вопросу о минимальной линейной интерполяции”, *Современные проблемы математики и информатики*, **9**, Ярославский государственный университет им. П. Г. Демидова, Ярославль, 2008, 31–37; [Nevskij M. V., Hlestkova I. V., “On minimal linear interpolation”, *Sovremennye problemy matematiki i informatiki*, **9**, P. G. Demidov Yaroslavl State University, Yaroslavl, 2008, 31–37, (in Russian).]
- [5] Невский М. В., “Об одном соотношении для минимальной нормы интерполяционного проектора”, *Модел. и анализ информ. систем*, **16:1** (2009), 24–43; [Nevskij M. V., “On a certain relation for the minimal norm of an interpolational projection”, *Modeling and Analysis of Information Systems*, **16:1** (2009), 24–43, (in Russian).]
- [6] Невский М. В., “Об одном свойстве n -мерного симплекса”, *Матем. заметки*, **87:4** (2010), 580–593; English transl.: Nevskii M. V., “On a property of n -dimensional simplices”, *Math. Notes*, **87:4** (2010), 543–555.

- [7] Невский М. В., *Геометрические оценки в полиномиальной интерполяции*, Ярославский государственный университет им. П. Г. Демидова, Ярославль, 2012; [Nevskii M. V., *Geometricheskie ocenki v polinomialnoy interpoliyacii*, P. G. Demidov Yaroslavl State University, Yaroslavl, 2012, (in Russian).]
- [8] Невский М. В., Ухалов А. Ю., “О числовых характеристиках симплекса и их оценках”, *Модел. и анализ информ. систем*, **23**:5 (2016), 602–618; [Nevskii M. V., Ukhalov A. Yu., “On numerical characteristics of a simplex and their estimates”, *Modeling and Analysis of Information Systems*, **23**:5 (2016), 602–618, (in Russian).]
- [9] Невский М. В., Ухалов А. Ю., “Новые оценки числовых величин, связанных с симплексом”, *Модел. и анализ информ. систем*, **24**:1 (2017), 34–50; [Nevskii M. V., Ukhalov A. Yu., “New estimates of numerical values related to a simplex”, *Modeling and Analysis of Information Systems*, **24**:1 (2017), 34–50, (in Russian).]
- [10] Невский М. В., Ухалов А. Ю., “Об n -мерных симплексах, удовлетворяющих включениям $S \subset [0, 1]^n \subset nS$ ”, *Модел. и анализ информ. систем*, **24**:5 (2017), 578–595; [Nevskii M. V., Ukhalov A. Yu., “On n -Dimensional Simplices Satisfying Inclusions $S \subset [0, 1]^n \subset nS$ ”, *Modeling and Analysis of Information Systems*, **24**:5 (2017), 578–595, (in Russian).]
- [11] Невский М. В., Ухалов А. Ю., “О минимальном коэффициенте поглощения для n -мерного симплекса”, *Модел. и анализ информ. систем*, **25**:1 (2018), 140–150; [Nevskii M. V., Ukhalov A. Yu., “On Minimal Absorption Index for an n -Dimensional Simplex”, *Modeling and Analysis of Information Systems*, **25**:1 (2018), 140–150, (in Russian).]
- [12] Сеге Г., *Ортогональные многочлены*, Гос. изд-во физ.-мат. литературы, М., 1962; Szego G., *Orthogonal Polynomials*, American Mathematical Society, New York, 1959, (in English).
- [13] Суетин П. К., *Классические ортогональные многочлены*, Наука, М., 1979; [Suetin P. K., *Klassicheskie ortogonalnye mnogochleny*, Nauka, Moscow, 1979, (in Russian).]
- [14] Холл М., *Комбинаторика*, Мир, М., 1970; Hall M., Jr, *Combinatorial theory*, Blaisdall publishing company, Waltham (Massachusetts)–Toronto–London, 1967, (in English).
- [15] Butzer P. L., Schmidt M., Stark E. L., “Observations on the history of central B -splines”, *Archive for History of Exact Sciences*, 1988, № 2, 137–156.
- [16] Comtet L., “Permutations by number of rises; Eulerian numbers”, *Advanced Combinatorics: The Art of Finite and Infinite Expansions*, Reidel, Dordrecht, Netherlands, 1974.
- [17] Ehrenborg R., Readdy M., Steingrimsson E., “Mixed volumes and slices of the cube”, *Journal of Combinatorial Theory. Series A.*, **81** (1998), 121–126.
- [18] Graham R. L., Knuth D. E., Patashnik O., *Concrete mathematics: A foundation for computer science*, Addison–Wesley, Reading, MA, 1994.
- [19] Hudelson M., Klee V., Larman D., “Largest j -simplices in d -cubes: some relatives of the Hadamard maximum determinant problem”, *Linear Algebra Appl.*, **241–243** (1996), 519–598.
- [20] de Laplace M., *Oeuvres complètes. V. 7*, Réédité par Gauthier–Villars, Paris, 1886.
- [21] Mangano S., *Mathematica cookbook*, O’Reilly Media Inc., Cambridge, 2010.
- [22] Nevskii M., “Properties of axial diameters of a simplex”, *Discrete Comput. Geom.*, **46**:2 (2011), 301–312.
- [23] Scott P. R., “Lattices and convex sets in space”, *Quart. J. Math. Oxford (2)*, **36** (1985), 359–362.
- [24] Scott P. R., “Properties of axial diameters”, *Bull. Austral. Math. Soc.*, **39** (1989), 329–333.
- [25] Sommerfeld A., “Eine besonders anschauliche Ableitung des Gaussischen Fehlergesetzes”, *Festschrift Ludwig Boltzmann gewidmet zum 60. Geburtstag*, 20. Februar, 1904, Barth, Leipzig, 1904.

- [26] Stanley R. P., "Eulerian partitions of a unit hypercube", *Higher Combinatorics*, Proceedings of the NATO Advanced Study Institute, Berlin, West Germany, September 1–10, 1976, Reidel, Dordrecht/Boston, 1977.

Nevskii M. V., Ukhalov A. Yu., "On Optimal Interpolation by Linear Functions on an n -Dimensional Cube", *Modeling and Analysis of Information Systems*, **25:3** (2018), 291–311.

DOI: 10.18255/1818-1015-2018-3-291-311

Abstract. Let $n \in \mathbb{N}$, and let Q_n be the unit cube $[0, 1]^n$. By $C(Q_n)$ we denote the space of continuous functions $f : Q_n \rightarrow \mathbb{R}$ with the norm $\|f\|_{C(Q_n)} := \max_{x \in Q_n} |f(x)|$, by $\Pi_1(\mathbb{R}^n)$ — the set of polynomials of n variables of degree ≤ 1 (or linear functions). Let $x^{(j)}$, $1 \leq j \leq n+1$, be the vertices of n -dimensional nondegenerate simplex $S \subset Q_n$. An interpolation projector $P : C(Q_n) \rightarrow \Pi_1(\mathbb{R}^n)$ corresponding to the simplex S is defined by equalities $Pf(x^{(j)}) = f(x^{(j)})$. The norm of P as an operator from $C(Q_n)$ to $C(Q_n)$ may be calculated by the formula $\|P\| = \max_{x \in \text{ver}(Q_n)} \sum_{j=1}^{n+1} |\lambda_j(x)|$. Here λ_j are the basic Lagrange polynomials with respect to S , $\text{ver}(Q_n)$ is the set of vertices of Q_n . Let us denote by θ_n the minimal possible value of $\|P\|$. Earlier, the first author proved various relations and estimates for values $\|P\|$ and θ_n , in particular, having geometric character. The equivalence $\theta_n \asymp \sqrt{n}$ takes place. For example, the appropriate, according to dimension n , inequalities may be written in the form $\frac{1}{4}\sqrt{n} < \theta_n < 3\sqrt{n}$. If the nodes of the projector P^* coincide with vertices of an arbitrary simplex with maximum possible volume, we have $\|P^*\| \asymp \theta_n$. When an Hadamard matrix of order $n+1$ exists, holds $\theta_n \leq \sqrt{n+1}$. In the paper, we give more precise upper bounds of numbers θ_n for $21 \leq n \leq 26$. These estimates were obtained with the application of maximum volume simplices in the cube. For constructing such simplices, we utilize maximum determinants containing the elements ± 1 . Also, we systematize and comment the best nowadays upper and low estimates of numbers θ_n for a concrete n .

Keywords: n -dimensional simplex, n -dimensional cube, interpolation, projector, norm, numerical methods

On the authors:

Mikhail V. Nevskii, orcid.org/0000-0002-6392-7618, Doctor of Science,
Centre of Integrable Systems, P.G. Demidov Yaroslavl State University,
14 Sovetskaya str., Yaroslavl, 150003, Russian Federation, e-mail: mnevsk55@yandex.ru

Alexey Yu. Ukhalov, orcid.org/0000-0001-6551-5118, PhD,
Centre of Integrable Systems, P.G. Demidov Yaroslavl State University,
14 Sovetskaya str., Yaroslavl, 150003, Russian Federation, e-mail: alex-ukhalov@yandex.ru

Acknowledgments:

This work was carried out within the framework of the state programme of the Ministry of Education and Science of the Russian Federation, project № 1.12873.2018/12.1

©Орешкина (Никольская) О. В., 2017

DOI: 10.18255/1818-1015-2018-3-312-322

УДК 512.7

О гипотезах Ходжа, Тэйта и Мамфорда–Тэйта для расслоенных произведений семейств регулярных поверхностей с геометрическим родом 1

Орешкина (Никольская) О. В.

получена 24 декабря 2017

Аннотация. Доказаны гипотезы Ходжа, Тэйта и Мамфорда–Тэйта для расслоенного произведения двух неизотривиальных 1-параметрических семейств регулярных поверхностей с геометрическим родом 1 при некоторых условиях на вырожденные слои, ранги групп Нерона–Севери общих геометрических слоёв семейств и представления групп Ходжа в трансцендентных частях рациональных когомологий.

Пусть $\pi_i : X_i \rightarrow C$ ($i = 1, 2$) – проективное неизотривиальное семейство поверхностей (возможно, с вырождениями) над гладкой проективной кривой C . Предположим, что дискриминантные локусы $\Delta_i = \{\delta \in C \mid \text{Sing}(X_{i\delta}) \neq \emptyset\}$ не пересекаются, $h^{2,0}(X_{ks}) = 1$, $h^{1,0}(X_{ks}) = 0$ для любого гладкого слоя X_{ks} , причём выполнены следующие условия:

(i) для любой точки $\delta \in \Delta_i$ и преобразования Пикара–Лефшеца $\gamma \in \text{GL}(H^2(X_{is}, \mathbb{Q}))$, ассоциированного с гладкой частью $\pi'_i : X'_i \rightarrow C \setminus \Delta_i$ морфизма π_i и с обходом вокруг точки $\delta \in C$, имеем неравенство $(\log(\gamma))^2 \neq 0$;

(ii) многообразия X_i ($i = 1, 2$), кривая C и структурные морфизмы $\pi_i : X_i \rightarrow C$ определены над некоторым конечнопорожденным подполем $k \hookrightarrow \mathbb{C}$.

Если для общих геометрических слоёв X_{1s} и X_{2s} выполнено хотя бы одно из следующих условий: (a) $b_2(X_{1s}) - \text{rank NS}(X_{1s})$ является нечетным числом, $b_2(X_{1s}) - \text{rank NS}(X_{1s}) \neq b_2(X_{2s}) - \text{rank NS}(X_{2s})$; (b) кольцо $\text{End}_{\text{Hg}(X_{1s})} \text{NS}_{\mathbb{Q}}(X_{1s})^{\perp}$ – мнимое квадратичное поле, $b_2(X_{1s}) - \text{rank NS}(X_{1s}) \neq 4$, $\text{End}_{\text{Hg}(X_{2s})} \text{NS}_{\mathbb{Q}}(X_{2s})^{\perp}$ – вполне вещественное поле или $b_2(X_{1s}) - \text{rank NS}(X_{1s}) > b_2(X_{2s}) - \text{rank NS}(X_{2s})$; (c) $[b_2(X_{1s}) - \text{rank NS}(X_{1s}) \neq 4, \text{End}_{\text{Hg}(X_{1s})} \text{NS}_{\mathbb{Q}}(X_{1s})^{\perp} = \mathbb{Q}; b_2(X_{1s}) - \text{rank NS}(X_{1s}) \neq b_2(X_{2s}) - \text{rank NS}(X_{2s})]$, то для расслоенного произведения $X_1 \times_C X_2$ верна гипотеза Ходжа, для любого гладкого проективного k -многообразия X_0 с условием $X_1 \times_C X_2 \xrightarrow{\sim} X_0 \otimes_k \mathbb{C}$ верны гипотеза Тэйта об алгебраических циклах и гипотеза Мамфорда–Тэйта для когомологий чётной степени. Более того, пространство $H_{\text{ét}}^2(X_0 \otimes_k \bar{k}, \mathbb{Q}_l(1))$ порождается классами дивизоров.

Ключевые слова: гипотезы Ходжа, Тэйта, Мамфорда–Тэйта, расслоенное произведение, группа Мамфорда–Тэйта, l -адическое представление

Для цитирования: Орешкина (Никольская) О. В., "О гипотезах Ходжа, Тэйта и Мамфорда–Тэйта для расслоенных произведений семейств регулярных поверхностей с геометрическим родом 1", *Моделирование и анализ информационных систем*, 25:3 (2018), 312–322.

Об авторах:

Орешкина (Никольская) Ольга Владимировна, orcid.org/0000-0002-6742-8453, канд. физ.-мат. наук, доцент, Владимирский государственный университет им. А.Г. и Н.Г. Столетовых, ул. Горького, 87, г. Владимир, 600000, Россия, e-mail: papichonok@yandex.ru

Благодарности:

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (грант № 16-31-00266).

Введение

Пусть X — гладкое проективное комплексное многообразие, $r \in \mathbb{Z}$, $r \geq 0$,

$$H^{2r}(X, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C} = \bigoplus_{p+q=2r} H^{p,q}(X, \mathbb{C})$$

— разложение Ходжа. Гипотеза Ходжа [1] утверждает, что $\mathbb{Q}$ -пространство

$$H^{2r}(X, \mathbb{Q}) \cap H^{r,r}(X, \mathbb{C})$$

порождается классами когомологий алгебраических циклов коразмерности r на X . Эта гипотеза верна для всех многообразий размерности ≤ 3 , для всех простых абелевых многообразий простой размерности [2], а также для некоторых других типов абелевых многообразий, перечисленных в обзоре [3], для гладких моделей расслоенных произведений некоторых неизотривиальных семейств $K3$ -поверхностей над гладкой проективной кривой [4], [5], [6].

С другой стороны, гипотеза Мамфорда–Тэйта утверждает, что для любого гладкого проективного многообразия X_0 над конечнопорождённым подполем $k \hookrightarrow \mathbb{C}$ алгебра Ли образа l -адического представления

$$\rho_l^{(n)} : \text{Gal}(\bar{k}/k) \rightarrow \text{GL}(H_{\text{ét}}^n(X_0 \otimes_k \bar{k}, \mathbb{Q}_l))$$

изоморфна алгебре Ли $\text{Lie MT}(H^n(X_0 \otimes_k \mathbb{C}, \mathbb{Q}))(\mathbb{Q}_l)$ группы l -адических точек группы Мамфорда–Тэйта $\text{MT}(H^n(X_0 \otimes_k \mathbb{C}, \mathbb{Q}))$ структуры Ходжа $H^n(X_0 \otimes_k \mathbb{C}, \mathbb{Q})$ [7], [8].

Эта гипотеза верна, например, для $K3$ -поверхностей [9] и абсолютно простых абелевых многообразий простой размерности [10], [11].

Наконец, гипотеза Тэйта об алгебраических циклах утверждает, что для любого гладкого проективного многообразия X_0 над конечнопорождённым полем k и любого простого числа $l \neq \text{char}(k)$ $\mathbb{Q}_l$ -пространство

$$H_{\text{ét}}^{2r}(X_0 \otimes_k k^s, \mathbb{Q}_l(r))^{\text{Gal}(k^s/k)}$$

порождается классами алгебраических циклов коразмерности r на X_0 [12].

Эта гипотеза верна для $K3$ -поверхностей [9], для абелевых многообразий над конечными и числовыми полями в случае $r = 1$ ([13], [14]), для абсолютно простых абелевых многообразий простой размерности над конечными полями [15], для регулярных поверхностей с геометрическим родом 1 — слоёв неизотривиального гладкого семейства — в случае $\text{char}(k) = 0$ [16].

Мы доказываем гипотезы Ходжа, Тэйта и Мамфорда–Тэйта для расслоенного произведения двух неизотривиальных 1-параметрических семейств регулярных поверхностей с геометрическим родом 1 при некоторых условиях на вырожденные слои, ранги групп Нерона–Севери общих геометрических слоёв семейств и представления групп Ходжа в трансцендентных частях рациональных когомологий.

Основными результатами являются теорема 1 и следствие 1.

Заметим, что в качестве гладких слоёв семейств могут быть $K3$ -поверхности, а также минимальные регулярные поверхности основного типа (размерности Кодаиры $\kappa = 2$) с геометрическим родом 1, принадлежащие одному из следующих типов: (а) поверхности с $K^2 \leq 2$; (б) поверхности с $3 \leq K^2 \leq 8$, модули которых лежат

в одной компоненте модулей с поверхностью Тодорова; (с) поверхности с $K^2 = 3$ с кручением группы Пикара $\mathbb{Z}/3\mathbb{Z}$.

Автор благодарит С.Г. Танкеева за внимательное прочтение рукописи и интересные обсуждения.

1. Отображение периодов и группы Ходжа

1.1. Типы гладких слоев семейств поверхностей

Пусть V – гладкая проективная поверхность основного типа над конечнопорожденным полем $k \hookrightarrow \mathbb{C}$ с $h^{2,0}(V \otimes_k \mathbb{C}) = 1$. Если минимальная модель поверхности $V \otimes_k \mathbb{C}$ принадлежит одному из следующих типов:

- (а) поверхности с $q = 0$ и $K^2 \leq 2$;
- (б) поверхности с $q = 0$ и $3 \leq K^2 \leq 8$, модули которых лежат в одной компоненте модулей с поверхностью Тодорова;
- (с) поверхности с $q = 0$ и $K^2 = 3$ с кручением группы Пикара $\mathbb{Z}/3\mathbb{Z}$;
- (d) поверхности с $q = 1$ и $K^2 = 2$;
- (е) поверхности с $q = 1$ и $K^2 = 3$ и общим слоем отображения Альбанезе рода 3;
- (f) поверхности с $q = 1$ и $K^2 = 4$ в любой из восьми компонент модулей, описанных в работе Пигнателли [17],

то можно считать, что существует такой гладкий проективный k -морфизм $f : \mathcal{X} \rightarrow \mathcal{S}$ над некоторой гладкой связной базой $\mathcal{S}$, что отображение периодов, ассоциированное с вариацией структур Ходжа $R^2 f_{*} \mathbb{Q}$, непостоянно, причём многообразие V является слоем морфизма f над некоторой точкой $s \in \mathcal{S}(k)$, гипотеза Тэйта для дивизоров на V и гипотеза Мамфорда–Тэйта для когомологий степени 2 верны [16, теорема 9.3].

1.2. Определение групп Ходжа и Мамфорда–Тэйта

Пусть S – гладкое проективное многообразие. Рассмотрим разложение Ходжа

$$H^n(S, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C} = \bigoplus_{p+q=n} H^{p,q}(S, \mathbb{C}),$$

где $H^{p,q}(S, \mathbb{C})$ – пространство гармонических форм типа (p, q) .

Пусть $U^1 = \{e^{i\theta} | \theta \in \mathbb{R}\}$ – единичная окружность. Определим ее действие в $H^n(S, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C}$ следующим образом: $e^{i\theta}$ действует на $H^{p,q}(S, \mathbb{C})$ как умножение на число $e^{i\theta(p-q)}$. В итоге мы получаем морфизм групп

$$U^1 \xrightarrow{h} \mathrm{GL}(H^n(S, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{R}).$$

Определение 1. Группой Ходжа структуры Ходжа $H^n(S, \mathbb{Q})$ называется наименьшая алгебраическая $\mathbb{Q}$ -подгруппа $\mathrm{Hg}(H^n(S, \mathbb{Q})) \hookrightarrow \mathrm{GL}(H^n(S, \mathbb{Q}))$, группа $\mathbb{R}$ -точек которой содержит $h(U^1)$.

По теореме Лефшеца о дивизорах имеем:

$$H^2(S, \mathbb{Q})^{\mathrm{Hg}(H^2(S, \mathbb{Q}))} = H^2(S, \mathbb{Q}) \cap H^{1,1}(S, \mathbb{C}) = \mathrm{NS}(S) \otimes_{\mathbb{Z}} \mathbb{Q} \stackrel{\mathrm{def}}{=} \mathrm{NS}_{\mathbb{Q}}(S),$$

где $\mathrm{NS}(S)$ – группа Нерона–Севери многообразия S .

Определим действие группы $\mathbb{C}^\times = \mathrm{Res}_{\mathbb{C}/\mathbb{R}}(G_m)(\mathbb{R})$ в $H^n(S, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C}$ следующим образом: элемент $z \in \mathbb{C}^\times$ действует на $H^{p,q}(S, \mathbb{C})$ как умножение на число $z^p \bar{z}^q$. В итоге получаем морфизм групп

$$\mathbb{C}^\times \xrightarrow{h} \mathrm{GL}(H^n(S, \mathbb{Q})) \otimes_{\mathbb{Q}} \mathbb{R}.$$

Определение 2. Группой Мамфорда–Тэйта $\mathrm{MT}(H^n(S, \mathbb{Q}))$ называется наименьшая алгебраическая $\mathbb{Q}$ -подгруппа $\mathrm{MT}(H^n(S, \mathbb{Q})) \hookrightarrow \mathrm{GL}(H^n(S, \mathbb{Q}))$, группа $\mathbb{R}$ -точек которой содержит $h(\mathbb{C}^\times)$.

Описание группы $\mathrm{Hg}(H^2(S, \mathbb{Q}))$ в случае, когда $h^{2,0}(S) = 1$, содержится в работе Ю.Г. Зархина [18].

1.3. Точки, общие в смысле Ходжа, непостоянное отображение периодов и бесконечная группа монодромии

Лемма 1. [19, п. 1.10]. Пусть $f : \mathcal{X} \rightarrow \mathcal{S}$ – гладкий проективный морфизм над гладкой связной комплексной кривой $\mathcal{S}$, слоями которого являются поверхности $\mathcal{X}_s$ с $h^{2,0}(\mathcal{X}_s) = 1$. Если отображение периодов, ассоциированное с вариацией структур Ходжа $R^2 f_* \mathbb{Q}$, непостоянно, то существует такое счётное подмножество $\Delta_{\mathrm{countable}} \subset \mathcal{S}$, что функция $s \mapsto \mathrm{rank} \mathrm{NS}(\mathcal{X}_s)$ постоянна на множестве $\mathcal{S} \setminus \Delta_{\mathrm{countable}}$.

По определению, $s \in \mathcal{S} \setminus \Delta_{\mathrm{countable}}$, если и только если связная компонента единицы замыкания в $\mathbb{Q}$ -топологии Зариского образа представления монодромии $\pi_1(\mathcal{S}, s) \rightarrow \mathrm{GL}(H^2(\mathcal{X}_s, \mathbb{Q}))$ является нормальной подгруппой группы Ходжа $\mathrm{Hg}(H^2(\mathcal{X}_s, \mathbb{Q}))$ [20, §0, теорема о нормальной подгруппе]. Такие точки s называются общими в смысле Ходжа.

Лемма 1 позволяет заменять выражение ”точка, общая в смысле Ходжа” на выражение ”общая геометрическая точка”, где ”общность” точки означает ее принадлежность множеству $\mathcal{S} \setminus \Delta_{\mathrm{countable}}$ для некоторого счётного подмножества $\Delta_{\mathrm{countable}} \hookrightarrow \mathcal{S}$.

Предложение 1. [20, §1, предложение 1.2]. Пусть $f : \mathcal{X} \rightarrow \mathcal{S}$ – гладкое проективное семейство поверхностей с $h^{2,0} = 1$. Тогда следующие условия эквивалентны:

а) отображение периодов голоморфной 2-формы не является отображением $\mathcal{S}$ в точку (другими словами, отображение периодов, ассоциированное с вариацией структур Ходжа $R^2 f_* \mathbb{Q}$, непостоянно);

б) образ представления монодромии $\pi_1(\mathcal{S}, s) \rightarrow \mathrm{GL}(H^2(\mathcal{X}_s, \mathbb{Q}))$ бесконечен.

Мы называем проективное семейство $f : \mathcal{X} \rightarrow \mathcal{S}$ гладких поверхностей, удовлетворяющее условиям предложения 1, *неизотривиальным*. Если $\bar{f} : \bar{\mathcal{X}} \rightarrow \bar{\mathcal{S}}$ – его компактификация, то семейство $\bar{f} : \bar{\mathcal{X}} \rightarrow \bar{\mathcal{S}}$ также называется неизотривиальным.

2. Доказательство основной теоремы

2.1. Формулировка основной теоремы

Теорема 1. Пусть $\pi_i : X_i \rightarrow C$ ($i = 1, 2$) – проективное неизотривиальное семейство поверхностей (возможно, с вырождениями) над гладкой проективной

кривой C . Предположим, что дискриминантные локусы

$$\Delta_i = \{\delta \in C \mid \text{Sing}(X_{i\delta}) \neq \emptyset\} \quad (i = 1, 2)$$

не пересекаются, $h^{2,0}(X_{ks}) = 1$, $h^{1,0}(X_{ks}) = 0$ для любого гладкого слоя X_{ks} , причём выполнены следующие условия:

(i) любой вырожденный слой $X_{i\delta} \subset X_i$ является объединением гладких неприводимых поверхностей кратности 1 с нормальными пересечениями и геометрическим родом 0 (случай сильного вырождения);

(ii) замыкание образа монодромии $\pi_1(C \setminus \Delta_i, s) \rightarrow \text{GL}(H^2(X_{is}, \mathbb{Q}))$ в топологии Зариского является связной $\mathbb{Q}$ -группой;

(iii) многообразия X_i ($i = 1, 2$), кривая C и структурные морфизмы $\pi_i : X_i \rightarrow C$ определены над некоторым конечнопорожденным подполем $k \hookrightarrow \mathbb{C}$.

Если для общих геометрических слоев X_{1s} и X_{2s} выполнено хотя бы одно из следующих условий:

- (a) $b_2(X_{1s}) - \text{rank NS}(X_{1s})$ является нечетным числом,
 $b_2(X_{1s}) - \text{rank NS}(X_{1s}) \neq b_2(X_{2s}) - \text{rank NS}(X_{2s})$;
- (b) кольцо $\text{End}_{\text{Hg}(X_{1s})} \text{NS}_{\mathbb{Q}}(X_{1s})^{\perp}$ – мнимое квадратичное поле,
 $b_2(X_{1s}) - \text{rank NS}(X_{1s}) \neq 4$,
 $\text{End}_{\text{Hg}(X_{2s})} \text{NS}_{\mathbb{Q}}(X_{2s})^{\perp}$ – вполне вещественное поле или
 $b_2(X_{1s}) - \text{rank NS}(X_{1s}) > b_2(X_{2s}) - \text{rank NS}(X_{2s})$;
- (c) $b_2(X_{1s}) - \text{rank NS}(X_{1s}) \neq 4$, $\text{End}_{\text{Hg}(X_{1s})} \text{NS}_{\mathbb{Q}}(X_{1s})^{\perp} = \mathbb{Q}$,
 $b_2(X_{1s}) - \text{rank NS}(X_{1s}) \neq b_2(X_{2s}) - \text{rank NS}(X_{2s})$,

то для расслоенного произведения $X_1 \times_C X_2$ верна гипотеза Ходжа, для любого гладкого проективного k -многообразия X_0 с условием $X_1 \times_C X_2 \xrightarrow{\sim} X_0 \otimes_k \mathbb{C}$ верны гипотеза Тэйта об алгебраических циклах и гипотеза Мамфорда–Тэйта для когомологий чётной степени. Более того, пространство $H_{\text{ét}}^2(X_0 \otimes_k \bar{k}, \mathbb{Q}_l(1))$ порождается классами дивизоров.

2.2. Морфизмы трансцендентных частей и представления монодромии

Положим $\Delta = \Delta_1 \cup \Delta_2$, $C' = C \setminus \Delta \xrightarrow{j} C$, $\pi'_i = \pi_i|_{\pi_i^{-1}(C')}$: $\pi_i^{-1}(C') \stackrel{\text{def}}{=} X'_i \rightarrow C'$, $\pi : X_1 \times_C X_2 \rightarrow C$ – структурный морфизм расслоенного произведения, $\pi' = \pi|_{\pi^{-1}(C')}$: $\pi^{-1}(C') \stackrel{\text{def}}{=} X' \rightarrow C'$.

Всюду в дальнейшем $G_i^{(2)}$ – замыкание в $\mathbb{Q}$ -топологии Зариского образа представления монодромии $\pi_1(C', s) \rightarrow \text{GL}(H^2(X_{is}, \mathbb{Q}))$.

Лемма 2. При выполнении условий теоремы 1 для общих геометрических слоёв X_{1s} , X_{2s} имеем:

$$\text{Hom}_{\pi_1(C', s)}(\text{NS}_{\mathbb{Q}}(X_{1s})^{\perp}, \text{NS}_{\mathbb{Q}}(X_{2s})^{\perp}) = 0.$$

Эта лемма доказана в [19, п. 2.3] для случая (a); в [5, лемма 2] для случая (b); в [6, п. 1.4] для случая (c).

2.3. Рациональные когомологии степени 2 и группы Нерона–Севери

Из леммы 2 легко получается следующий результат:

Лемма 3. [19, п. 2.8]. *Имеем: $H^2(X_k, \mathbb{Q}) = \text{NS}_{\mathbb{Q}}(X_k)$, $H^2(X, \mathbb{Q}) = \text{NS}_{\mathbb{Q}}(X)$.*

Кроме того, согласно сильной теореме Лефшеца $H^4(X_k, \mathbb{Q}) = H^2(X_k, \mathbb{Q}) \cup \text{cl}_{X_k}(H_k)$, где H_k – гиперплоское сечение многообразия X_k . Поэтому из леммы 3 следует, что пространство $H^4(X_k, \mathbb{Q})$ порождается алгебраическими классами когомологий.

2.4. Доказательство основной теоремы

Пусть

$$f : Z \rightarrow \pi^{-1}(\Delta)$$

– нормализация схемы $\pi^{-1}(\Delta)$. Тогда Z – несвязное объединение гладких неприводимых компонент дивизора $\pi^{-1}(\Delta)$. Поскольку $f : Z \rightarrow \pi^{-1}(\Delta)$ – разрешение особенностей замкнутой подсхемы $i_{\Delta} : \pi^{-1}(\Delta) \hookrightarrow X$, то имеется точная последовательность смешанных $\mathbb{Q}$ -структур Ходжа [21, следствие (8.2.8)]:

$$H^2(Z, \mathbb{Q}) \xrightarrow{(i_{\Delta}f)_*} H^4(X, \mathbb{Q}) \rightarrow H^4(X', \mathbb{Q}),$$

где $(i_{\Delta}f)_*$ – морфизм бистепени $(1, 1)$ смешанных структур Ходжа. Поэтому

$$(i_{\Delta}f)_* H^2(Z, \mathbb{Q}) = \text{Ker} [H^4(X, \mathbb{Q}) \rightarrow H^4(X', \mathbb{Q})].$$

Действуя по алгоритму п. 2.8 в [19], легко проверить, что имеется точная последовательность

$$0 \rightarrow (i_{\Delta}f)_* \text{NS}_{\mathbb{Q}}(Z) \rightarrow [H^4(X, \mathbb{Q}) \cap H^{2,2}(X, \mathbb{C})] \rightarrow H^0(C', R^4\pi'_*\mathbb{Q}) \rightarrow 0,$$

в которой пространство $H^0(C', R^4\pi'_*\mathbb{Q})$ порождается образами алгебраических классов на X . Значит, для X верна гипотеза Ходжа об алгебраических циклах.

С другой стороны, поскольку пространство $H^0(C', R^4\pi'_*\mathbb{Q})$ порождается образами алгебраических классов на X , то из точности последовательности рациональных структур Ходжа [19, формула (2.16)]

$$0 \rightarrow (i_{\Delta}f)_* H^2(Z, \mathbb{Q}) \rightarrow H^4(X, \mathbb{Q}) \rightarrow H^0(C', R^4\pi'_*\mathbb{Q}) \rightarrow 0$$

следует, что

$$\text{Hg}(H^4(X, \mathbb{Q})) = \text{Hg}((i_{\Delta}f)_* H^2(Z, \mathbb{Q}))$$

в силу тривиальности действия окружности U^1 на алгебраических классах когомологий типа $(2, 2)$, поэтому согласно [3, лемма B.53] имеем

$$\begin{aligned} \text{MT}(H^4(X, \mathbb{Q})) &= G_m \cdot \text{Hg}(H^4(X, \mathbb{Q})) = G_m \cdot \text{Hg}((i_{\Delta}f)_* H^2(Z, \mathbb{Q})) = \\ &= \text{MT}((i_{\Delta}f)_* H^2(Z, \mathbb{Q})). \end{aligned}$$

Значит, достаточно доказать гипотезу Мамфорда–Тэйта для когомологий степени 2 многообразия Z , являющегося несвязным объединением произведений вида

$S \times T$ или $T \times S$, где S – гладкая проективная поверхность с геометрическим родом 0, T – гладкая регулярная поверхность с геометрическим родом 1.

Заметим, что в силу формулы Кюннета $H^2(S \times T, \mathbb{Q}) = H^2(S, \mathbb{Q}) \oplus H^2(T, \mathbb{Q})$, потому что $H^1(T, \mathbb{Q}) = 0$.

С другой стороны, $p_g(S) = 0$, поэтому $H^2(S, \mathbb{Q})$ порождается классами дивизоров. Значит, гипотеза Мамфорда–Тэйта для когомологий четной степени сводится к гипотезе Мамфорда–Тэйта для поверхности T , а этот случай следует из результатов Моонена [16, теорема 9.3].

Наконец, хорошо известно, что из гипотезы Мамфорда–Тэйта для когомологий X_0 четной степени следует эквивалентность доказанной выше гипотезы Ходжа для $X_1 \times_{\mathbb{C}} X_2 = X_0 \otimes_k \mathbb{C}$ и гипотезы Тэйта для X_0 (с учётом леммы 3).

2.5. Следствие из основной теоремы

Следствие 1. Пусть $\pi_i : X_i \rightarrow C$ ($i = 1, 2$) – проективное неизотривиальное семейство поверхностей (возможно, с вырождениями) над гладкой проективной кривой C . Предположим, что дискриминантные локусы

$$\Delta_i = \{\delta \in C \mid \text{Sing}(X_{i\delta}) \neq \emptyset\} \quad (i = 1, 2)$$

не пересекаются, $h^{2,0}(X_{ks}) = 1$, $h^{1,0}(X_{ks}) = 0$ для любого гладкого слоя X_{ks} , причём выполнены следующие условия:

(i) для любой точки $\delta \in \Delta_i$ и преобразования Пикара–Лефшеца

$$\gamma \in \text{GL}(H^2(X_{is}, \mathbb{Q})),$$

ассоциированного с гладкой частью $\pi'_i : X'_i \rightarrow C \setminus \Delta_i$ морфизма π_i и с обходом вокруг точки $\delta \in C$, имеем неравенство $(\log(\gamma))^2 \neq 0$;

(ii) многообразия X_i ($i = 1, 2$), кривая C и структурные морфизмы $\pi_i : X_i \rightarrow C$ определены над некоторым конечнопорожденным подполем $k \hookrightarrow \mathbb{C}$.

Если для общих геометрических слоев X_{1s} и X_{2s} выполнено хотя бы одно из следующих условий:

- (a) $b_2(X_{1s}) - \text{rank NS}(X_{1s})$ является нечетным числом,
 $b_2(X_{1s}) - \text{rank NS}(X_{1s}) \neq b_2(X_{2s}) - \text{rank NS}(X_{2s})$;
- (b) кольцо $\text{End}_{\text{Hg}(X_{1s})} \text{NS}_{\mathbb{Q}}(X_{1s})^{\perp}$ – мнимое квадратичное поле,
 $b_2(X_{1s}) - \text{rank NS}(X_{1s}) \neq 4$,
 $\text{End}_{\text{Hg}(X_{2s})} \text{NS}_{\mathbb{Q}}(X_{2s})^{\perp}$ – вполне вещественное поле или
 $b_2(X_{1s}) - \text{rank NS}(X_{1s}) > b_2(X_{2s}) - \text{rank NS}(X_{2s})$;
- (c) $[b_2(X_{1s}) - \text{rank NS}(X_{1s}) \neq 4, \text{End}_{\text{Hg}(X_{1s})} \text{NS}_{\mathbb{Q}}(X_{1s})^{\perp} = \mathbb{Q}]$,
 $b_2(X_{1s}) - \text{rank NS}(X_{1s}) \neq b_2(X_{2s}) - \text{rank NS}(X_{2s})$,

то для расслоенного произведения $X_1 \times_C X_2$ верна гипотеза Ходжа, для любого гладкого проективного k -многообразия X_0 с условием $X_1 \times_C X_2 \xrightarrow{\sim} X_0 \otimes_k \mathbb{C}$ верны гипотеза Тэйта об алгебраических циклах и гипотеза Мамфорда–Тэйта для когомологий четной степени. Более того, пространство $H_{\text{et}}^2(X_0 \otimes_k \bar{k}, \mathbb{Q}_l(1))$ порождается классами дивизоров.

Доказательство. Пусть D^* – проколотый диск на C с центром $\delta \in \Delta_i$. Фундаментальная группа $\pi_1(D^*, s) \xrightarrow{\sim} \mathbb{Z}$ действует на когомологиях общего слоя X_{is} , $s \in D^*$.

Обозначим через $\gamma \in \mathrm{GL}(H^2(X_{is}, \mathbb{Q}))$ образ образующей группы $\pi_1(D^*, s)$, называемый *преобразованием Пикара–Лефшеца* или *локальным преобразованием монодромии*.

По условию следствия преобразование Пикара–Лефшеца γ удовлетворяет условию $N^2 \neq 0$, где $N = \log(\gamma)$. Это свойство сохраняется при переходе к подходящей гладкой проективной модели схемы $X_i \times_C \tilde{C}$ над $\tilde{C}$, где $\tilde{C} \rightarrow C$ – произвольное определённое над k разветвлённое накрытие кривой C . Действительно, можно считать, что отображение $\tilde{C} \rightarrow C$ индуцирует отображение проколотых дисков $\tilde{D}^* \rightarrow D^*$, задаваемое формулой $t = \tau^n$ в локальных координатах t и τ на C и $\tilde{C}$ соответственно (так, что точка δ задается уравнением $t = 0$). Морфизм $\tilde{D}^* \rightarrow D^*$ не разветвлён, имеет степень n и определяет вложение $\pi_1(\tilde{D}^*, \tilde{s}) \hookrightarrow \pi_1(D^*, s)$, поэтому $\tilde{\gamma} = \gamma^n$. Остаётся заметить, что $\log(\gamma^n) = n \log(\gamma)$, так что $(\log(\tilde{\gamma}))^2 \neq 0$.

Используя в случае необходимости такую замену базы $\tilde{C} \rightarrow C$, мы можем считать, что выполнено условие (ii) теоремы 1.

Проверим, что в рассматриваемом случае можно считать выполненным условие (i) теоремы 1.

Действительно, в силу теоремы Мамфорда о полустабильных редукциях [22, с. 53–54] мы можем считать, что все вырожденные слои морфизма $\pi_i : X_i \rightarrow C$ являются объединениями гладких неприводимых поверхностей кратности 1 с нормальными пересечениями.

Пусть $X_{i\delta} = V_1 + \dots + V_n$, где V_j – неприводимая компонента дивизора $X_{i\delta}$. Тогда по теореме Вик. С. Куликова [23, теорема 2.7] имеем:

$$p_g(X_{is}) = \sum_{j=1}^n p_g(V_j) + \frac{1}{2} \mathrm{ckh}^1 + h^2(\Pi(X_{i\delta})), \quad (2.1)$$

где в рассматриваемом случае

$$\begin{aligned} p_g(X_{is}) &\stackrel{\mathrm{def}}{=} h^{2,0}(X_{is}) = \dim_{\mathbb{C}} H^0(X_{is}, \Omega_{X_{is}}^2) = 1, \\ p_g(V_j) &\stackrel{\mathrm{def}}{=} h^{2,0}(V_j) = \dim_{\mathbb{C}} H^0(V_j, \Omega_{V_j}^2), \\ \mathrm{ckh}^1 &\stackrel{\mathrm{def}}{=} \dim_{\mathbb{Q}} \mathrm{Coker} \left(\bigoplus_i H^1(V_i, \mathbb{Q}) \rightarrow \bigoplus_{i < j} H^1(V_i \cap V_j, \mathbb{Q}) \right), \\ h^2(\Pi(X_{i\delta})) &\stackrel{\mathrm{def}}{=} \dim H^2(\Pi(X_{i\delta})), \end{aligned}$$

$\Pi(X_{i\delta})$ – полиэдр, ассоциированный с вырождением $X_{i\delta} = V_1 + \dots + V_n$. Кроме того, $N^2 = (\log(\gamma))^2 = 0$ тогда и только тогда, когда $h^2(\Pi(X_{i\delta})) = 0$ [23, теорема 2.7, (a)].

В нашем случае $N^2 \neq 0$, поэтому $h^2(\Pi(X_{i\delta})) \neq 0$. В силу формулы (2.1) и равенства $p_g(X_{is}) = 1$ имеем равенства $p_g(V_j) = 0$ для всех j . Значит, выполнено условие (i) теоремы 1.

Остаётся заметить, что если $W \rightarrow V$ – сюръективный k -морфизм гладких проективных k -многообразий, то из гипотезы Мамфорда–Тэйта для когомологий чётной степени многообразия W следует гипотеза Мамфорда–Тэйта для когомологий

чётной степени многообразия V [24, следствие 4.4]. Это доказывает следствие 1, потому что из гипотезы Мамфорда–Тэйта для X_0 следует эквивалентность доказанной выше гипотезы Ходжа для $X_1 \times_C X_2 = X_0 \otimes_k \mathbb{C}$ и гипотезы Тэйта для X_0 . $\square$

Замечание 1. Предположим, что общий слой $X_{k\eta}$ морфизма $\pi_k : X_k \rightarrow C$ ($k = 1, 2$) имеет размерность Кодaira $\kappa(X_{k\eta}) = 2$ (другими словами, является поверхностью основного типа) и род кривой C больше 1. Тогда для расслоенного произведения $X = X_1 \times_C X_2$ имеем в силу теоремы Каваматы [25, теорема 2] и теоремы Биркара [26, теорема 1.3]:

$$\kappa(X) \geq \kappa(X_{1\eta} \times_{\kappa(\eta)} X_{2\eta}) + \kappa(C) \geq \kappa(X_{1\eta}) + \kappa(X_{2\eta}) + \kappa(C) = 5,$$

так что в рассматриваемом случае многообразие X является многообразием основного типа.

Список литературы

- [1] Hodge W. V. D., “The topological invariants of algebraic varieties”, *Proceedings of International Congress of Mathematicians*, **1**, 1952, 182–192.
- [2] Танкеев С. Г., “Циклы на простых абелевых многообразиях простой размерности”, *Изв. АН СССР. Сер. матем.*, **46**:1 (1982), 155–170; English transl.: Tankeev S. G., “Cycles on simple abelian varieties of prime dimension”, *Mathematics of the USSR–Izvestiya*, **20**:1 (1983), 157–171.
- [3] Gordon B. B., “A survey of the Hodge conjecture for Abelian varieties”, Appendix in: Lewis J. D., *A survey of the Hodge conjecture. 2 ed.*, CRM Monograph Series, **10**, American Mathematical Society, Providence, RI, 1999, 297–356.
- [4] Никольская О. В., “Об алгебраических циклах на расслоенном произведении семейств КЗ поверхностей”, *Изв. РАН. Сер. матем.*, **77**:1 (2013), 145–164; English transl.: Nikolskaya O. V., “On algebraic cycles on a fibre product of families of K3 surfaces”, *Izv. Math.*, **77**:1 (2013), 143–162.
- [5] Никольская О. В., “О геометрии гладкой модели расслоенного произведения семейств КЗ поверхностей”, *Матем. сб.*, **205**:2 (2014), 123–130; English transl.: Nikolskaya O. V., “On the geometry of a smooth model of a fibre product of families of K3 surfaces”, *Sbornik: Mathematics*, **205**:2 (2014), 269–276.
- [6] Никольская О. В., “Об алгебраических классах когомологий на гладкой модели расслоенного произведения семейств КЗ поверхностей”, *Матем. заметки*, **96**:5 (2014), 738–746; English transl.: Nikolskaya O. V., “On algebraic cohomology classes on a smooth model of a fiber product of families of K3 surfaces”, *Math. Notes*, **96**:5 (2014), 745–752.
- [7] Mumford D., “Families of abelian varieties”, *Proc. of Symposium in Pure Math. AMS*, **IX** (1966), 347–351.
- [8] Serre J.-P., “Representations l-adiques”, *Algebraic number theory*, Papers contributed for the International Symposium, Kyoto, 1976, ed. S. Iyanaga, Japan Society for the Promotion of Science, Tokyo, 1977, 177–193.
- [9] Танкеев С. Г., “Поверхности типа КЗ над числовыми полями и гипотеза Мамфорда–Тэйта. II”, *Изв. РАН. Сер. матем.*, **59**:3 (1995), 179–206; English transl.: Tankeev S. G., “Surfaces of K3 type over number fields and the Mumford-Tate conjecture. II”, *Russian Akad. Sci. Izv. Math.*, **59**:3 (1995), 619–646.
- [10] Танкеев С. Г., “Циклы на простых абелевых многообразиях простой размерности над числовыми полями”, *Изв. АН СССР. Сер. матем.*, **31**:6 (1987), 1214–1227; English transl.: Tankeev S. G., “Cycles on simple abelian varieties of prime dimension over number fields”, *Mathematics of the USSR–Izvestiya*, **31**:3 (1988), 527–540.

- [11] Pink R., “ l -adic algebraic monodromy group cocharacters, and the Mumford-Tate conjecture”, *J. reine. angew. Math.*, **495** (1998), 187–237.
 - [12] Tate J., “Algebraic cycles and poles of zeta functions”, *Arithmetical Algebraic Geometry*, Proc. Conf. Purdue Univ., 1963, Harper and Row, New York, 1965, 93–110.
 - [13] Tate J., “Endomorphisms of abelian varieties over finite fields”, *Invent. Math.*, **2** (1966), 134–144.
 - [14] Faltings G., “Endlichkeitssätze für abelsche Varietäten über Zahlkörpern”, *Invent. Math.*, **73**:3 (1983), 349–366.
 - [15] Танкеев С. Г., “О циклах на абелевых многообразиях простой размерности над конечными и числовыми полями”, *Изв. АН СССР. Сер. матем.*, **47**:2 (1983), 356–365; English transl.: Tankeev S. G., “On cycles on abelian varieties of prime dimension over finite and number fields”, *Mathematics of the USSR–Izvestiya*, **22**:2 (1984), 329–337.
 - [16] Moonen B., “On the Tate and Mumford-Tate conjectures in codimension one for varieties with $h^{2,0} = 1$ ”, *Duke Math. J.*, **166**:4 (2017), 739–799.
 - [17] Pignatelli R., “Some (big) irreducible components of the moduli space of minimal surfaces of general type with $p_g = q = 1$ and $K^2 = 4$ ”, *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl.*, **20**:3 (2009), 207–226.
 - [18] Zarhin Yu. G., “Hodge groups of $K3$ surfaces”, *Journal für die reine und angewandte Mathematik*, **341** (1983), 193–220.
 - [19] Никольская О. В., “Об алгебраических циклах на расслоенных произведениях неизотривиальных семейств регулярных поверхностей с геометрическим родом 1”, *Моделирование и анализ информационных систем*, **23**:4 (2016), 440–465; [Nikol’skaya O. V., “On algebraic cycles on fibre products of non-isotrivial families of regular surfaces with geometric genus 1”, *Model. Anal. Inform. Sist.*, **23**:4 (2016), 440–465, (in Russian).]
 - [20] Мустафин Г. А., “Семейства алгебраических многообразий и инвариантные циклы”, *Изв. АН СССР. Сер. матем.*, **49**:5 (1985), 948–978; English transl.: Mustafin G. A., “Families of algebraic varieties and invariant cycles”, *Mathematics of the USSR–Izvestiya*, **27**:2 (1986), 251–278.
 - [21] Deligne P., “Théorie de Hodge. III”, *Inst. Hautes Études Sci. Publ. Math.*, **44** (1974), 5–77.
 - [22] Kempf G. et al., *Toroidal embeddings. I*, Lecture Notes in Mathematics, **339**, Springer-Verlag, Berlin – New York, 1973.
 - [23] Куликов Вик. С., “Вырождения $K3$ -поверхностей и поверхностей Энриквеса”, *Изв. АН СССР. Сер. матем.*, **41**:5 (1977), 1008–1042; English transl.: Kulikov Vic. S., “Degenerations of $K3$ surfaces and Enriques surfaces”, *Math. USSR–Izv.*, **11**:5 (1977), 957–988.
 - [24] Танкеев С. Г., “Об арифметике и геометрии общего гиперповерхностного сечения”, *Изв. РАН. Сер. матем.*, **66**:2 (2002), 173–204; English transl.: Tankeev S. G., “The arithmetic and geometry of a generic hypersurface section”, *Izv. Math.*, **66**:2 (2002), 393–424.
 - [25] Kawamata Y., “Kodaira dimension of algebraic fiber spaces over curves”, *Invent. Math.*, **66**:1 (1982), 57–71.
 - [26] Birkar C., “Iitaka conjecture $C_{n,m}$ in dimension six”, *Compositio Mathematica*, **2009**:6 (1979), 1442–1446.
-

Oreshkina (Nikol'skaya) O. V., "On the Hodge, Tate and Mumford-Tate Conjectures for Fibre Products of Families of Regular Surfaces with Geometric Genus 1", *Modeling and Analysis of Information Systems*, **25:3** (2018), 312–322.

DOI: 10.18255/1818-1015-2018-3-312-322

Abstract. The Hodge, Tate and Mumford-Tate conjectures are proved for the fibre product of two non-isotrivial 1-parameter families of regular surfaces with geometric genus 1 under some conditions on degenerated fibres, the ranks of the Néron - Severi groups of generic geometric fibres and representations of Hodge groups in transcendental parts of rational cohomology.

Let $\pi_i : X_i \rightarrow C$ ($i = 1, 2$) be a projective non-isotrivial family (possibly with degeneracies) over a smooth projective curve C . Assume that the discriminant loci $\Delta_i = \{\delta \in C \mid \text{Sing}(X_{i\delta}) \neq \emptyset\}$ ($i = 1, 2$) are disjoint, $h^{2,0}(X_{ks}) = 1$, $h^{1,0}(X_{ks}) = 0$ for any smooth fibre X_{ks} , and the following conditions hold:

(i) for any point $\delta \in \Delta_i$ and the Picard-Lefschetz transformation $\gamma \in \text{GL}(H^2(X_{i\delta}, \mathbb{Q}))$, associated with a smooth part $\pi'_i : X'_i \rightarrow C \setminus \Delta_i$ of the morphism π_i and with a loop around the point $\delta \in C$, we have $(\log(\gamma))^2 \neq 0$;

(ii) the variety X_i ($i = 1, 2$), the curve C and the structure morphisms $\pi_i : X_i \rightarrow C$ are defined over a finitely generated subfield $k \hookrightarrow \mathbb{C}$.

If for generic geometric fibres X_{1s} and X_{2s} at least one of the following conditions holds:

(a) $b_2(X_{1s}) - \text{rank NS}(X_{1s})$ is an odd prime number, $b_2(X_{1s}) - \text{rank NS}(X_{1s}) \neq b_2(X_{2s}) - \text{rank NS}(X_{2s})$;

(b) the ring $\text{End}_{\text{Hg}(X_{1s})} \text{NS}_{\mathbb{Q}}(X_{1s})^{\perp}$ is an imaginary quadratic field, $b_2(X_{1s}) - \text{rank NS}(X_{1s}) \neq 4$, $\text{End}_{\text{Hg}(X_{2s})} \text{NS}_{\mathbb{Q}}(X_{2s})^{\perp}$ is a totally real field or $b_2(X_{1s}) - \text{rank NS}(X_{1s}) > b_2(X_{2s}) - \text{rank NS}(X_{2s})$;

(c) $[b_2(X_{1s}) - \text{rank NS}(X_{1s}) \neq 4, \text{End}_{\text{Hg}(X_{1s})} \text{NS}_{\mathbb{Q}}(X_{1s})^{\perp} = \mathbb{Q}; \quad b_2(X_{1s}) - \text{rank NS}(X_{1s}) \neq b_2(X_{2s}) - \text{rank NS}(X_{2s})$,

then for the fibre product $X_1 \times_C X_2$ the Hodge conjecture is true, for any smooth projective k -variety X_0 with the condition $X_1 \times_C X_2 \xrightarrow{\sim} X_0 \otimes_k \mathbb{C}$ the Tate conjecture on algebraic cycles and the Mumford-Tate conjecture for cohomology of even degree are true.

Keywords: Hodge, Tate and Mumford-Tate conjectures, fibre product, Mumford-Tate group, l -adic representation

On the authors:

Olga V. Oreshkina (Nikol'skaya), orcid.org/0000-0002-6742-8453, PhD,
 A.G. and N.G. Stoletov Vladimir State University,
 87 Gorky str., Vladimir, 600000, Russia, e-mail: papichonok@yandex.ru.

Acknowledgments:

This work was supported by the Russian Foundation for Basic Research under the Grant No 16-31-00266.

Теория функций

©Морозов А. Н., 2018

DOI: 10.18255/1818-1015-2018-3-323-330

УДК 517.5

О дифференцируемости по Тейлору в пространствах L_p , $0 < p \leq \infty$

Морозов А. Н.

получена 15 января 2018

Аннотация. Функция $f \in L_p[I]$, $p > 0$, называется (k, p) -дифференцируемой в точке $x_0 \in I$, если существует алгебраический многочлен π степени не больше k , для которого выполняется $\|f - \pi\|_{L_p[J_h]} = o(h^{k+\frac{1}{p}})$, где $J_h = [x_0 - h; x_0 + h] \cap I$. Во внутренней точке при $k = 1$ и $p = \infty$ это равносильно определению обычной дифференцируемости функции. Имеется стандартная «иерархия» существования дифференциалов: если $p_1 < p_2$, то из (k, p_2) -дифференцируемости следует (k, p_1) -дифференцируемость. В работах С.Н. Бернштейна, А.П. Кальдерона и А. Зигмунда были даны приложения такой конструкции к построению описания функциональных пространств ($p = \infty$) и изучению локальных свойств решений дифференциальных уравнений ($1 \leq p \leq \infty$) соответственно. Данная статья связана с первой указанной работой. В статье вводится понятие равномерной дифференцируемости. Назовём (k, p) -дифференцируемую во всех точках отрезка I функцию f равномерно (k, p) -дифференцируемой на I , если для любого числа $\varepsilon > 0$ найдется число $\delta > 0$ такое, что для каждой точки $x \in I$ выполняется $\|f - \pi\|_{L_p[J_h]} < \varepsilon \cdot h^{k+\frac{1}{p}}$ при $0 < h < \delta$, $J_h = [x-h; x+h] \cap I$, где π – многочлен из условия (k, p) -дифференцируемости в точке x . На основе методов локальных приближений функций алгебраическими многочленами показано, что из равномерной (k, p) -дифференцируемости функции f при некотором $1 \leq p \leq \infty$ следует $f \in C^k[I]$. Следовательно, в таком случае дифференциалы «эквивалентны». Поскольку каждая функция из $C^k[I]$ является равномерно (k, p) -дифференцируемой на отрезке I при $1 \leq p \leq \infty$, то получаем определённый критерий принадлежности функции этому пространству. Диапазон $0 < p < 1$, очевидно, может быть включён в необходимое условие принадлежности функции $C^k[I]$, однако достаточность дифференцируемости по Тейлору в этом диапазоне пока в полной мере не доказана.

Ключевые слова: дифференцируемость функции по Тейлору, локальные приближения функций

Для цитирования: Морозов А. Н., "О дифференцируемости по Тейлору в пространствах L_p , $0 < p \leq \infty$ ", *Моделирование и анализ информационных систем*, **25:3** (2018), 323–330.

Об авторах:

Морозов Анатолий Николаевич, orcid.org/0000-0001-9940-159X канд. физ.-мат. наук, доцент,
Ярославский государственный университет им. П.Г. Демидова,
ул. Советская, 14, г. Ярославль, 150003, Россия, e-mail: moroz@uniyar.ac.ru

1. Введение и основные обозначения

Как обычно, $L_p[I]$ обозначает пространство действительных функций, интегрируемых в степени p ($0 < p < \infty$) по Лебегу на отрезке $I = [a; b]$, с величиной

элементов

$$\|f\|_{L_p[I]} = \left(\int_I |f(x)|^p dx \right)^{\frac{1}{p}};$$

при $p = \infty$ всюду ниже рассматривается $C[I]$ – пространство непрерывных на отрезке I функций с чебышевской нормой.

Когда неясность исключена, сокращаем обозначения до L_p и $\|f\|_p$ или соответственно до C и $\|f\|_\infty$. Длину I обозначаем $|I|$.

Также используются

$W_p^k = W_p^k[I] = \left\{ f : f^{(k-1)} \text{ абсолютно непрерывна на отрезке } I, f^{(k)} \in L_p[I] \right\}$,
 $k \in \mathbb{N}$, $1 \leq p < \infty$, и (при $p = \infty$) $C^k = C^k[I]$ – пространство k раз непрерывно дифференцируемых на отрезке I функций, – с нормами $\|f\|_p + \|f^{(k)}\|_p$.

Определение 1. Функция $f \in L_p[I]$, $0 < p \leq \infty$, называется (k, p) -дифференцируемой в точке $x_0 \in I$, если существует алгебраический многочлен π степени не больше k , для которого выполняется $\|f - \pi\|_{L_p[J_h]} = o(h^{k+\frac{1}{p}})$, где $J_h = [x_0 - h; x_0 + h] \cap I$.

Такой многочлен может быть только один. Во внутренней точке x_0 при $k = 1$ и $p = \infty$ определение равносильно обычной дифференцируемости (существованию производной), однако в общем случае из (k, ∞) -дифференцируемости в точке не следует существование k -й производной. Классическим примером является функция

$$f(x) = \begin{cases} x^{k+1} \sin(\frac{1}{x^k}), & x \neq 0, \\ 0, & x = 0; \end{cases}$$

которая (l, ∞) -дифференцируема (следовательно, (l, p) -дифференцируема при $0 < p \leq \infty$) в точке 0 для $l = 1, \dots, k$, но имеет лишь одну обычную производную. Также отметим, что несмотря на естественную «иерархию» существования дифференциалов (если $p_1 < p_2$, то из (k, p_2) -дифференцируемости следует (k, p_1) -дифференцируемость), примеры показывают их качественную близость для достаточно «хороших» функций. Так, функция $f(x) = |x|^\alpha$ является $(1, p)$ -дифференцируемой в нуле только для $\alpha > 1$ при $0 < p \leq \infty$.

Важные приложения данного понятия рассматривались, например, в работах С.Н. Бернштейна [1] / $p = \infty$ /, А.П. Кальдерона и А. Зигмунда [2] / $1 \leq p \leq \infty$ /. Настоящая статья связана с первой работой.

Для $f \in L_p[I]$ и $J \subseteq I$ обычным образом определяется

$$E_k(f; J)_p = \inf \{ \|f - \pi\|_{L_p[J]} : \pi \in P_k \}$$

– наилучшее приближение функции f алгебраическими многочленами степени не выше $k-1$ (порядка k) в $L_p[J]$. Если J не совпадает с I , то такое приближение называют локальным.

Из работы П.Л. Чебышева ([3], с. 23) следует, что если $f \in C[a; b]$ и в точке $x_0 \in (a; b)$ функция f имеет k -ю производную, то

$$\lim_{h \rightarrow 0} \frac{E_k(f; [x_0 - h; x_0 + h])_\infty}{(2h)^k} = \frac{1}{k! 2^{2k-1}} |f^{(k)}(x_0)|. \quad (1)$$

Бернштейн [1], развивая данный результат, показал, что для существования предела достаточно (k, ∞) -дифференцируемости в точке x_0 , а затем выразил «глобальные» дифференциальные свойства функции при помощи «разделённых локальных приближений». Его формулировка такова.

Теорема 1. Условие, необходимое и достаточное для того, чтобы непрерывная функция f имела непрерывную производную порядка k во всех точках отрезка $[a; b]$, заключается в том, что

$$\frac{E_k(f, [\alpha; \beta])_\infty}{(\beta - \alpha)^k} \rightarrow \varphi(x), \quad a \leq \alpha < x < \beta \leq b,$$

равномерно по x при $\alpha \rightarrow x$, $\beta \rightarrow x$, где непрерывная функция φ определяется равенством

$$k! 2^{2k-1} \varphi(x) = |f^{(k)}(x)|.$$

Пусть $m \in \mathbf{N}$. Рассмотрим разбиение τ_m полуинтервала $I = [a; b)$ на m полуинтервалов равной длины. По заданной функции $f \in L_p[I]$, $0 < p \leq \infty$, и разбиению τ_m построим ступенчатую функцию, определяемую формулой

$$\varphi_m^k(f)_p = \frac{E_k(f, J)_p}{c_{k,p} |J|^{k+\frac{1}{p}}}, \quad \text{при } x \in J,$$

на каждом $J \in \tau_m$, где в правой части применяется константа $c_{k,p} = E_k\left(\frac{x^k}{k!}, [0; 1]\right)_p$. В статьях [4] и [5] автором показано, что условие теоремы Бернштейна сводится к равномерной сходимости последовательности $\{\varphi_m^k(f)_\infty\}$, и аналогичное описание может быть дано для пространств W_p^k . Также показано, что рассмотрение последовательностей $\{\varphi_m^k(f)_q\}$ с переменным индексом q , $1 \leq q \leq \infty$, позволяет осуществлять переход к пространствам с другой нормой, поскольку характер сходимости этих последовательностей является инвариантом относительно q . Вот суммарный результат.

Теорема 2. Для того, чтобы функция f из L_q , $1 \leq q \leq \infty$, принадлежала пространству W_p^k , необходимо и достаточно, чтобы последовательность функций $\{\varphi_m^k(f)_q\}$ сходилась в пространстве L_p . При этом предельная функция совпадает с $|f^{(k)}|$.

Наряду с функцией $\varphi_m^k(f)_p$ будем рассматривать

$$U_m^k(f, I)_p = \inf \left\{ \|f - s_k\|_{L_p[I]} : s_k|_{J \in \tau_m} \in P_k \right\} = \left(\sum_{J \in \tau_m} E_k(f, J)_p^p \right)^{\frac{1}{p}}$$

— наилучшее приближение функции f в пространстве $L_p[I]$ кусочно-полиномиальными функциями степени не выше $k-1$ с интервалами полиномиальности из τ_m ;

$$U_m^k(f, I)_\infty = \max_{J \in \tau_m} E_k(f, J)_\infty.$$

Между $U_m^k(f)_p$ и величиной функции $\varphi_m^k(f)_p$ имеется прямая зависимость —

$$\frac{m^k}{|I|^k} U_m^k(f, I)_p = c_{k,p} \|\varphi_m^k(f)_p\|_{L_p[I]}, \quad (2)$$

сразу вытекающая из определений.

Следствие. Для $f \in W_p^k[I]$ выполняется

$$\lim_{m \rightarrow \infty} m^k U_m^k(f, I)_p = c_{k,p} |I|^k \|f^{(k)}\|_{L_p[I]}.$$

Определим далее для $0 < p \leq \infty$ обычные L_p -модули гладкости –

$$\omega_k(f, t)_p = \sup_{0 < h < t} \|\Delta_h^k f\|_{L_p[a; b-kh]}, \quad \text{где } \Delta_h^k f(x) = \sum_{i=0}^k (-1)^{k-i} \binom{k}{i} f(x + ih).$$

Пусть

$$H_p^k = \left\{ f \in L_p : \sup_{t>0} t^{-k} \omega_k(f, t)_p < \infty \right\}.$$

Как показал Ю.А. Брудный [6], [7], пространства H_p^k при $1 < p < \infty$ совпадают с W_p^k , а $H_1^k = \{f : f \in W_1^{(k-1)}, f^{(k-1)} \text{ имеет ограниченную вариацию}\}$. (Следовательно, пополнение C^k по норме

$$\|\cdot\|_p + \sup_{t>0} t^{-k} \omega_k(\cdot, t)_p$$

даёт W_p^k .) При $0 < p < 1$ другое описание H_p^k неизвестно.

2. Равномерная (k, p) -дифференцируемость

Покажем сначала, что формула (1) распространяется на все рассматриваемые значения p и для существования предела достаточно дифференцируемости функции по Тейлору в данной точке.

Лемма. При $0 < p \leq \infty$ для каждого I выполняется $E_k\left(\frac{x^k}{k!}, I\right)_p = c_{k,p} |I|^{k+\frac{1}{p}}$.

Доказательство. Используя замену переменной, переводящую $[a; b]$ в $[0; 1]$, существование многочлена наилучшего приближения и свойства E_k , при всех $0 < p \leq \infty$ получаем

$$E_k(x^k, [a; b])_p = (b-a)^{\frac{1}{p}} E_k\left((b-a)x + a\right)_p^{(k)} = (b-a)^{k+\frac{1}{p}} E_k(x^k, [0; 1])_p.$$

Лемма доказана.

Введём обозначение $\Lambda_p^k f(x_0) = k! a_k$, где a_k – коэффициент при степени k многочлена из условия (k, p) -дифференцируемости функции f в точке x_0 . Для краткости далее пишем $p_* = \min\{p; 1\}$.

Предложение 1. Если функция f является (k, p) -дифференцируемой ($p > 0$) во внутренней точке x_0 отрезка I , то

$$\lim_{h \rightarrow 0} \frac{E_k(f, [x_0 - h; x_0 + h])_p}{c_{k,p} (2h)^{k+\frac{1}{p}}} = |\Lambda_p^k f(x_0)|.$$

Доказательство. Пусть $\pi(x) = a_0 + a_1x + \dots + a_kx^k$, $J_h = [x_0 - h; x_0 + h]$, и выполняется $\|f - \pi\|_{L_p[J_h]} = o(h^{k+\frac{1}{p}})$. Из леммы, применённой к $J = J_h$, следует

$$\begin{aligned} & \left| \left(\frac{E_k(f, J)_p}{c_{k,p} |J|^{k+\frac{1}{p}}} \right)^{p*} - (k!|a_k|)^{p*} \right| = \frac{|E_k(f, J)_p^{p*} - E_k(a_kx^k, J)_p^{p*}|}{(c_{k,p} |J|^{k+\frac{1}{p}})^{p*}} \leq \\ & \leq \left(\frac{E_k(f(x) - a_kx^k, J)_p}{c_{k,p} |J|^{k+\frac{1}{p}}} \right)^{p*} = \left(\frac{E_k(f - \pi, J)_p}{c_{k,p} |J|^{k+\frac{1}{p}}} \right)^{p*} \leq \left(\frac{\|f - \pi\|_{L_p[J]}}{c_{k,p} |J|^{k+\frac{1}{p}}} \right)^{p*} \rightarrow 0 \end{aligned}$$

при $|J| \rightarrow 0$.

Определение 2. Назовём (k, p) -дифференцируемую во всех точках отрезка I функцию f равномерно (k, p) -дифференцируемой на I , если для любого числа $\varepsilon > 0$ найдется число $\delta > 0$ такое, что для каждой точки $x \in I$ выполняется $\|f - \pi\|_{L_p[J_h]} < \varepsilon \cdot h^{k+\frac{1}{p}}$ при $0 < h < \delta$, $J_h = [x - h; x + h] \cap I$, где π – многочлен из условия (k, p) -дифференцируемости в точке x .

Для такой функции f определена функция $\Lambda_p^k f$.

Теорема 3. Если функция f равномерно (k, p) -дифференцируема на I при некотором $0 < p \leq \infty$, то последовательность $\{\varphi_m^k(f)_p\}$ сходится равномерно на I к функции $|\Lambda_p^k f|$.

Доказательство. Рассмотрим произвольную точку $x_0 \in I$ и некоторое разбиение τ_m . Пусть полуинтервал $J = [x_{i-1}; x_i)$ из τ_m содержит точку x_0 , a_k – коэффициент при степени k многочлена π из условия (k, p) -дифференцируемости функции f в точке x_0 . Положим $h = \max\{x_0 - x_{i-1}, x_i - x_0\}$, тогда $h \leq |J| \leq 2h$. Рассуждая, как в предложении 1, получаем

$$\begin{aligned} & \left| (\varphi_m^k(f)_p(x_0))^{p*} - |\Lambda_p^k f(x_0)|^{p*} \right| = \left| \left(\frac{E_k(f, J)_p}{c_{k,p} |J|^{k+\frac{1}{p}}} \right)^{p*} - (k!|a_k|)^{p*} \right| \leq \\ & \leq \left(\frac{E_k(f - \pi, J)_p}{c_{k,p} |J|^{k+\frac{1}{p}}} \right)^{p*} \leq \left(\frac{\|f - \pi\|_{L_p[J]}}{c_{k,p} |J|^{k+\frac{1}{p}}} \right)^{p*} \leq \left(\frac{\|f - \pi\|_{L_p[J_h]}}{c_{k,p} h^{k+\frac{1}{p}}} \right)^{p*}. \end{aligned}$$

Здесь $J_h = [x_0 - h; x_0 + h] \cap I$. Поскольку $|J| = \frac{|I|}{m}$, то условие теоремы влечёт равномерную сходимость последовательности $\{\varphi_m^k(f)_p\}$ к $|\Lambda_p^k f|$.

Следствие. Если функция f удовлетворяет условию теоремы 3 при некотором $p \geq 1$, то $f \in C^k[I]$, $\Lambda_p^k f = f^{(k)}$.

Утверждение автоматически следует из объединения результатов теорем 2 и 3.

Отметим, из полученного результата вытекает такой факт: если при некотором значении $p \geq 1$ функция f равномерно (k, p) -дифференцируема на I , то в каждой точке $x_0 \in I$ коэффициент a_l , $l = 0, 1, \dots, k$, – при степени l многочлена π из условия (k, p) -дифференцируемости f в точке x_0 , – совпадает с $\frac{f^{(l)}(x_0)}{l!}$.

Любая функция f из $C^k[I]$ является, конечно, равномерно (k, p) -дифференцируемой на I при всех $0 < p \leq \infty$. Это легко выводится, например, из хорошо известной

формулы для остаточного члена разложения k раз дифференцируемой функции (форма Лагранжа)

$$f(x) = f(x_0) + f'(x_0)(x - x_0) + \dots + \frac{f^{(k-1)}(x_0)}{(k-1)!}(x - x_0)^{k-1} + \frac{f^{(k)}(\xi)}{k!}(x - x_0)^k,$$

где точка ξ заключена между x_0 и x . Последнее слагаемое можно записать в виде

$$\frac{f^{(k)}(x_0)}{k!}(x - x_0)^k + \alpha(x - x_0) \cdot (x - x_0)^k, \text{ где } \alpha(x - x_0) = \frac{f^{(k)}(\xi) - f^{(k)}(x_0)}{k!}.$$

Из непрерывности $f^{(k)}$ следует, что все функции $\alpha(x - x_0)$ можно одновременно ограничить сколь угодно малым положительным числом ε для любых точек x_0 и x из I , удалённых друг от друга не больше, чем на соответствующее число δ .

Таким образом, получаем определённый критерий принадлежности функции пространству C^k . Возвращаясь к вопросу о соотношении дифференциалов, видим, что равномерная (k, p) -дифференцируемость ($p \geq 1$) функции f на I влечёт равномерную (k, ∞) -дифференцируемость, т.е. дифференциалы в такой ситуации «эквивалентны».

Пространства $L_p, 0 < p < 1$, гораздо меньше изучены. Распространяется ли на них теорема 2, на данный момент неизвестно (см. [8]), поэтому выводы в этих случаях не являются завершёнными.

Предложение 2. Если функция f равномерно (k, p) -дифференцируема на I при некотором $0 < p < 1$, то $f \in H_p^k[I]$, $|\Lambda_p^k f| \in C[I]$, и выполняется

$$\lim_{m \rightarrow \infty} m^k U_m^k(f, I)_p = c_{k,p} |I|^k \|\Lambda_p^k f\|_p.$$

Доказательство. По теореме 3 последовательность $\{\varphi_m^k(f)_p\}$ (ступенчатых функций с условием «смещения узлов») сходится равномерно к $|\Lambda_p^k f|$. Предположив, что $|\Lambda_p^k f|$ не является непрерывной функцией, получим противоречие.

Существование предела в утверждении теоремы сразу следует из равенства (2).

Делаем вывод – последовательность $\{m^k U_m^k(f, I)_p\}$ ограничена, т.е. для некоторого M при всех m выполняется неравенство

$$U_m^k(f, I)_p \leq \frac{M}{m^k}.$$

В работе И.П. Иродовой [9] доказано при всех $0 < p \leq \infty$, что если для некоторой степенной (и даже более общего вида) функции ψ выполняется $U_m^k(\cdot, I)_p \leq \psi\left(\frac{1}{m}\right)$, то $\omega_k(\cdot, t)_p \leq \beta \psi(t)$ с постоянной β , зависящей от $k, p, |I|$. Получается

$$\omega_k(f, t)_p \leq \beta M t^k,$$

т.е. $f \in H_p^k$.

Предложение доказано.

В заключение отметим, что классическое понятие «равномерной непрерывности» получается в шкале «равномерной (k, p) -дифференцируемости» при $k = 0$. Этот факт граничит с несколькими другими, поэтому заслуживает отдельного рассмотрения.

Список литературы / References

- [1] Бернштейн С. Н., “К вопросу о локальном наилучшем приближении функций”, *Докл. АН СССР*, **26**:9 (1940), 839–842; [Bernstein S. N., “On the Question of Local Best Approximation of Functions”, *Dokl. USSR Acad. Sci.*, **26**:9 (1940), 839–842, (in Russian).]
- [2] Calderon A. P., Zygmund A., “Local properties of solution of elliptic partial differential equation”, *Studia Math.*, **20** (1961), 171–225.
- [3] Чебышев П. Л., *Собрание сочинений*, В 5 т. Т. 2, Изд. АН СССР, М.-Л., 1947; [Chebyshev P. L., *Collected Works*, In 5 v. V. 2, Izd. AN SSSR, Moscow–Leningrad, 1954, (in Russian).]
- [4] Морозов А. Н., “Аналог теоремы Бернштейна в пространстве L_1 ”, *Матем. заметки*, **57**:5 (1995), 699–703; English transl.: Morozov A. N., “Analog of Bernstein’s Theorem in the Space L_1 ”, *Math. Notes*, **57**:5 (1995), 485–488.
- [5] Морозов А. Н., “Об одном описании пространств дифференцируемых функций”, *Матем. заметки*, **70**:5 (2001), 758–768; English transl.: Morozov A. N., “On a Characterization of Spaces of Differentiable Functions”, *Math. Notes*, **70**:5 (2001), 688–697.
- [6] Брудный Ю. А., “Критерии существования производных в L^p ”, *Математический сборник*, **73**:1 (1967), 42–64; English transl.: Brudnyi Yu. A., “Criteria for the Existence of Derivatives in L^p ”, *Mathematics of the USSR-Sbornik*, **2**:1 (1967), 35–55.
- [7] Брудный Ю. А., “Пространства, определяемые с помощью локальных приближений”, *Тр. ММО*, **24** (1971), 69–132; English transl.: Brudnyi Yu. A., “Spaces Defined by Means of Local Approximations”, *Trans. Moscow Math. Soc.*, **24** (1971), 73–139.
- [8] Морозов А. Н., “Локальные приближения дифференцируемых функций”, *Мат. заметки*, **100**:2 (2016), 248–255; English transl.: Morozov A. N., “Local Approximations of Differentiable Functions”, *Math. Notes*, **100**:2 (2016), 256–262.
- [9] Иродова И. П., “Свойства функций, заданных скоростью убывания кусочно-полиномиальной аппроксимации”, *Исследования по теории функций многих вещественных переменных*, Сб. науч. трудов, Ярославль, 1980, 92–117; [Irodova I. P., “Svoystva funktsiy, zadannykh skorostyu ubyvaniya kusochno-polinomialnoy approksimatsii”, *Issledovaniya po teorii funktsiy mnogikh veshchestvennykh peremennykh*, Sb. nauch. trudov, Yaroslavl, 1980, 92–117, (in Russian).]

Morozov A. N., “On the Taylor Differentiability in Spaces L_p , $0 < p \leq \infty$ ”, *Modeling and Analysis of Information Systems*, **25**:3 (2018), 323–330.

DOI: 10.18255/1818-1015-2018-3-323-330

Abstract. The function $f \in L_p[I]$, $p > 0$, is called (k, p) -differentiable at a point $x_0 \in I$ if there exists an algebraic polynomial of π of degree no more than k for which holds $\|f - \pi\|_{L_p[J_h]} = o(h^{k+\frac{1}{p}})$, where $J_h = [x_0 - h; x_0 + h] \cap I$. At an internal point for $k = 1$ and $p = \infty$ this is equivalent to the usual definition of the function differentiability. At an interior point for $k = 1$ and $p = \infty$, the definition is equivalent to the usual differentiability of the function. There is a standard “hierarchy” for the existence of differentials (if $p_1 < p_2$, then (k, p_2) -differentiability should be (k, p_1) -differentiability.) In the works of S.N. Bernstein, A.P. Calderon and A. Zygmund were given applications of such a construction to build a description of functional spaces ($p = \infty$) and the study of local properties of solutions of differential equations ($1 \leq p \leq \infty$), respectively. This article is related to the first mentioned work. The article introduces the concept of uniform differentiability. We say that a function f , (k, p) -differentiable at all points of the segment I , is uniformly (k, p) -differentiable on I if for any number $\varepsilon > 0$ there is a number $\delta > 0$ such that for each point $x \in I$ runs $\|f - \pi\|_{L_p[J_h]} < \varepsilon \cdot h^{k+\frac{1}{p}}$ for $0 < h < \delta$, $J_h = [x - H; x + h] \cap I$, where π is the polynomial of the terms of the (k, p) -differentiability at the point x . Based on the methods of local approximations of functions by algebraic polynomials it is shown that a uniform (k, p) -differentiability of the function f at some $1 \leq p \leq \infty$ implies $f \in C^k[I]$. Therefore, in this case the

differentials are "equivalent". Since every function from $C^k[I]$ is uniformly (k, p) -differentiable on the interval I at $1 \leq p \leq \infty$, we obtain a certain criterion of belonging to this space. The range $0 < p < 1$, obviously, can be included into the necessary condition the membership of the function $C^k[I]$, but the sufficiency of Taylor differentiability in this range has not yet been fully proven.

Keywords: Taylor differentiability of function, local approximations of functions

On the authors:

Anatoly N. Morozov, orcid.org/0000-0001-9940-159X, PhD,

P.G. Demidov Yaroslavl State University,

14 Sovetskaya str., Yaroslavl, 150003, Russia, e-mail: moroz@uniyar.ac.ru

©Климов В. С., 2018

DOI: 10.18255/1818-1015-2018-3-331-342

УДК 517.518

Изопериметрические и функциональные неравенства

Климов В. С.

получена 3 января 2018

Аннотация. Устанавливаются оценки снизу интегрального функционала

$$\int_{\Omega} f(u(x), \nabla u(x)) dx,$$

где Ω – ограниченная область в пространстве $\mathbb{R}^n$ ($n \geq 2$), интегрант $f(t, p)$ ($t \in [0, \infty)$, $p \in \mathbb{R}^n$) – функция, B -измеримая по переменному t и выпуклая и четная по переменному p , $\nabla u(x)$ – градиент (в смысле Соболева) функции $u: \Omega \rightarrow \mathbb{R}$. В первом и втором разделах существенную роль играют свойства перестановок дифференцируемых функций, а также изопериметрическое неравенство вида $H^{n-1}(\partial A) \geq \lambda(m_n A)$, связывающее $(n-1)$ -мерную меру Хаусдорфа $H^{n-1}(\partial A)$ относительной границы ∂A множества $A \subset \Omega$ с его n -мерной мерой Лебега $m_n A$. Интегрант f при этом предполагается изотропным, т.е. $f(t, p) = f(t, q)$, если $|p| = |q|$. Намечены приложения установленных результатов к многомерным вариационным задачам.

Для функций u , обращающихся в нуль на границе области Ω , предположение об изотропности f можно опустить. В этом случае существенную роль начинают играть операции симметризации по Штейнеру и Шварцу интегранта f и функции u . Соответствующие варианты оценок снизу обсуждаются в третьем пункте. Принципиально новым здесь является то, что операция симметризации применяется не только к функции u , но и к интегранту f . Геометрическую основу результатов третьего пункта составляют неравенство Брунна–Минковского, а также свойства симметризации алгебраической суммы множеств.

Ключевые слова: перестановка, выпуклая функция, мера, градиент, симметризация, изопериметрическое неравенство

Для цитирования: Климов В. С., "Изопериметрические и функциональные неравенства", *Моделирование и анализ информационных систем*, **25:3** (2018), 331–342.

Об авторах:

Климов Владимир Степанович, orcid.org/0000-0001-9560-8315, д-р физ.-мат. наук, профессор, Ярославский государственный университет им. П.Г. Демидова, ул. Советская, 14, г. Ярославль, 150003 Российская Федерация, e-mail: VSK76@list.ru

1. Перестановки функций

Начало теории перестановок относится к работам Я. Штейнера и Г. Шварца, в которых изучались симметризации множеств и симметричные перестановки функций.

Эти исследования были продолжены в трудах Г. Харди и Г. Литтлвуда, рассматривавших перестановки функций и последовательностей. В конце 30-х годов прошлого века сложилось новое направление в математике – теория вложения пространств Соболева. Первые результаты этой теории были получены с помощью симметричных перестановок. В последующие два десятилетия основным в теории вложения стал метод интегральных представлений. Лишь отдельные функциональные неравенства (оценки емкостей, площадей поверхности, основной частоты упругой мембраны, жёсткости кручения и т.п.) устанавливались с помощью методов симметризации [1]. Возрождение интереса к геометрическим методам произошло в 1960 г., когда В.Г. Мазья и независимо Федерер и Флеминг переоткрыли тесную связь теорем вложения с изопериметрическими неравенствами. Ряд важных результатов, полученных методами геометрической теории меры и относящихся к пространствам Соболева, содержится в монографии [2]. Подробное изложение истории вопроса и значительную библиографию можно найти в [1] – [10].

Пусть Ω – измеримое подмножество $\mathbb{R}^n$, n -мерная лебегова мера m_n которого конечна и положительна: $0 < a = m_n \Omega < \infty$. Если $u: \Omega \rightarrow \mathbb{R}$ измеримая почти везде конечная функция, то при любом действительном t множество $A_t := \{x \in \Omega : |u(x)| > t\}$ измеримо. Функция $\mu(t) := m_n(A_t)$ ($0 \leq t < \infty$) называется *функцией распределения* u . Функция $\bar{u}(s)$ одного переменного s , определенная при $s \in [0, a)$ равенством $\bar{u}(s) = \inf\{\tau : m_n A_\tau \leq s\}$, называется *перестановкой* u . (Если множество $\{\tau : m_n A_\tau \leq 0\}$ пусто, то $\bar{u}(0) = \infty$). Положим

$$\bar{u}(a) = \lim_{s \rightarrow a-0} \bar{u}(s).$$

Функция $\bar{u}$ характеризуется свойствами: $\bar{u}$ не возрастает, непрерывна справа и равноизмерима с функцией $u: \Omega \rightarrow \mathbb{R}$ в том смысле, что $\mu(\tau) = m_n\{s : \bar{u}(s) > \tau\}$. Для непрерывности $\bar{u}$ достаточно, чтобы функция распределения строго возрастала на $[\bar{u}(a), \bar{u}(0)]$. Отметим равенства $\bar{u}(a) = \text{vrai} \min |u|$, $\bar{u}(0) = \text{vrai} \max |u|$.

Всюду далее Ω есть ограниченная область в $\mathbb{R}^n$. Введем обозначения: ∂M – граница множества $M \subset \mathbb{R}^n$, $H^{n-1}(M)$ – $(n-1)$ -мерная мера Хаусдорфа множества M . Важную роль в дальнейшем играет изопериметрическое неравенство

$$H^{n-1}(\partial A \cap \Omega) \geq \lambda(m_n A), \quad (1)$$

где A – любое подмножество Ω с локально липшицевой внутренней относительно Ω частью границы, $\lambda: [0, a] \rightarrow [0, \infty)$ – функция на $[0, a]$, возрастающая на $\left[0, \frac{a}{2}\right]$ и

$\lambda(s) = \lambda(a-s) \forall s \in [0, a]$. Задача о поиске максимальной функции λ , удовлетворяющей оценке (1), достаточно сложна и решена лишь для отдельных областей. Как показано в [2], всегда можно считать, что $\lambda(s) > 0$ при $s \in (0, a)$. Обозначим через $J(\lambda)$ класс областей Ω , для которых неравенство (1) верно с функцией $\lambda(\cdot)$, непрерывной на $[0, a]$, возрастающей и положительной на $(0, a/2]$ и $\lambda(s) = \lambda(a-s)$. Класс областей, для которых функция λ удовлетворяет неравенству $\lambda(s) \geq k_0 s^\alpha$ ($k_0 > 0, 0 < 2s < a$), обозначаем символом J_α . Этот класс был введен и исследован в работах В.Г. Мазья.

Области, удовлетворяющие условию конуса, принадлежат классу J_α с $\alpha = 1 - \frac{1}{n}$ [2].

Обозначим через $W_1^1(\Omega)$ совокупность локально суммируемых в Ω функций, имеющих в Ω суммируемые производные (в смысле С.Л. Соболева [3]) первого порядка. В $W_1^1(\Omega)$ введём норму [2]

$$\|u; W_1^1(\Omega)\| = \int_{\Omega} \nabla_1 u(x) dx + \int_{\omega} |u(x)| dx.$$

Здесь ω – некоторое фиксированное (непустое) открытое множество с компактным замыканием $\bar{\omega} \subset \Omega$, $\nabla u(x)$ – градиент функции $u(x)$, $\nabla_1 u(x)$ – евклидова длина вектора $\nabla u(x)$. Относительно данной нормы $W_1^1(\Omega)$ – сепарабельное банахово пространство. Множество функций класса $W_1^1(\Omega) \cap C^\infty(\Omega)$ плотно в пространстве $W_1^1(\Omega)$ [2], [5]. Пространство $W_1^1(\Omega)$ вложено в пространство $L^m(\Omega)$, $m \geq 1$, в том и только том случае, если $\Omega \in J_{1/m}$ [2, гл. 3].

Ниже применяется следующий вариант формулы коплощади ([2], [5]).

Предложение 1. Пусть $\mathbb{D}$ – открытое множество в $\mathbb{R}^n$, u – вещественная функция класса $C^1(\mathbb{D})$, причем $\nabla_1 u(x) > 0 \forall x \in \mathbb{D}$; $\mathbb{B}_t := \{x \in \mathbb{D}, |u(x)| = t\}$, $g \in L(\mathbb{D})$. Тогда для почти всех значений $t \geq 0$ функция $\frac{g}{\nabla_1 u}$ интегрируема по $\mathbb{B}_t$ относительно $(n-1)$ -мерной меры Хаусдорфа dH^{n-1} , соответствующий интеграл

$$\int_{\mathbb{B}_t} \frac{g(x)}{\nabla_1 u(x)} dH^{n-1}$$

суммируем по мере dt и имеет место формула

$$\int_{\mathbb{D}} g(x) dx = \int_0^\infty dt \int_{\mathbb{B}_t} \frac{g(x)}{\nabla_1 u(x)} dH^{n-1}. \quad (2)$$

Далее используются обозначения: $\theta = (0, 0, \dots, 0) \in \mathbb{R}^n$, символы $\blacktriangleleft$ и $\blacktriangleright$ – начало и конец доказательства.

Лемма 1. Пусть $\Omega \in J(\lambda)$, $u \in W_1^1(\Omega)$, $\gamma(\cdot)$ – неотрицательная измеримая по Борелю функция на $[0, \infty)$. Тогда

$$\int_{\Omega} \gamma(|u(x)|) \nabla_1 u(x) dx \geq \int_0^\infty \gamma(t) \lambda(m_n A_t) dt, \quad (3)$$

где $A_t = \{x \in \Omega : |u(x)| > t\}$.

$\blacktriangleleft$ Установим (3), предполагая вначале функцию $\gamma(\cdot)$ непрерывной и ограниченной на $[0, \infty)$ ($0 \leq \gamma(t) < \gamma_0 < \infty \forall t \in [0, \infty)$). Фиксируем последовательность $u_i(x)$ функций класса $W_1^1(\Omega) \cap C^\infty(\Omega)$, сходящуюся к функции $u(x)$ в метрике $W_1^1(\Omega)$. Пусть $A_t^i = \{x \in \Omega : |u_i(x)| > t\}$, $B_t^i = \{x \in \Omega : |u_i(x)| = t\}$. Поскольку u_i – функция класса $C^\infty(\Omega)$, то почти при всех $t > 0$ множество B_t^i есть $(n-1)$ -мерное многообразие класса C^∞ . В силу предложения 1 и неравенства (1) имеем

$$\int_{\Omega} \gamma(|u_i(x)|) \nabla_1 u_i(x) dx = \int_{\nabla_1 u(x) > 0} \gamma(|u_i(x)|) \nabla_1 u_i(x) dx \geq \int_0^\infty \gamma(t) \lambda(m_n A_t^i) dt. \quad (4)$$

Так как последовательность u_i сходится к u в метрике $W_1^1(\Omega)$, то u_i сходится к u по мере, $m_n(A_t^i \Delta A_t) \rightarrow 0$ при $i \rightarrow \infty$ и почти при всех t , следовательно,

$$\lim_{i \rightarrow \infty} \int_0^\infty \gamma(t) \lambda(m_n A_t^i) dt = \int_0^\infty \gamma(t) \lambda(m_n A_t) dt.$$

Последовательность $\gamma(|u_i|) \nabla_1 u_i$ сходится по мере к функции $\gamma(|u|) \nabla_1 u$. В силу ограниченности функции $\gamma(\cdot)$ функции $\gamma(|u_i|) \nabla_1 u_i$ имеют равномерно абсолютно непрерывные интегралы. Поэтому

$$\lim_{i \rightarrow \infty} \int_\Omega \gamma(|u_i(x)|) \nabla_1 u_i(x) dx = \int_\Omega \gamma(|u(x)|) \nabla_1 u(x) dx.$$

Теперь (3) следует из (4) и теоремы Фату.

Отбросим теперь условие непрерывности функции $\gamma(t)$, предположение её ограниченности пока остается, так что $0 \leq \gamma(t) < \gamma_0 < \infty$. Как известно, существует такая неотрицательная функция $\alpha(\cdot)$ класса $L[0, \infty)$, что для любого измеримого по Борелю множества $B \subset \mathbb{R}_+$ справедливо равенство [5]

$$\int_{|u|^{-1}(B)} \nabla_1 u(x) = \int_B \alpha(t) dt. \quad (5)$$

Фиксируем $\varepsilon > 0$ и подберем $\delta > 0$ так, чтобы выполнялось неравенство

$$\int_{|u|^{-1}(B)} \nabla_1 u(x) = \int_B \alpha(t) dt < \varepsilon$$

для любого измеримого по Борелю множества B , для которого $m_1 B < \delta$.

По теореме Лузина существует такое замкнутое множество $T \subset \mathbb{R}_+ = [0, \infty)$, что $m_1(\mathbb{R}_+ \setminus T) < \delta$ и сужение функции $\gamma(\cdot)$ на T непрерывно. Пусть $\gamma_1(t)$ – функция, совпадающая с $\gamma(\cdot)$ на множестве T и линейная на интервалах дополнительных к T . Очевидно, что функция $\gamma_1(\cdot)$ непрерывна и ограничена на $\mathbb{R}_+$;

$$m_1\{t \in \mathbb{R}_+ : \gamma(t) \neq \gamma_1(t)\} < \delta, \quad 0 \leq \gamma_1(t) < \gamma_0.$$

Согласно доказанной части леммы справедливы неравенства

$$\int_\Omega \gamma_1(|u(x)|) \nabla_1 u(x) dx \geq \int_0^\infty \gamma_1(t) \lambda(m_n A_t) dt \geq \int_T \gamma(t) \lambda(m_n A_t) dt.$$

Оценим левую часть полученного неравенства сверху

$$\begin{aligned} \int_\Omega \gamma_1(|u(x)|) \nabla_1 u(x) dx &\leq \int_\Omega \gamma(|u(x)|) \nabla_1 u(x) dx + \gamma_0 \int_{|u(x)| \notin T} \nabla_1 u(x) dx \leq \\ &\leq \int_\Omega \gamma(u(x)) \nabla_1 u(x) dx + \varepsilon \gamma_0. \end{aligned}$$

Так как δ, ε могут быть взяты сколь угодно малыми, равенство (3) в рассматриваемом случае установлено.

Откажемся теперь от предположения ограниченности функции γ . Для любого натурального числа N функция $\gamma^N(t) = \min\{\gamma(t), N\}$ измерима по Борелю и ограничена сверху. Справедлива цепь соотношений

$$\int_{\Omega} \gamma(|u(x)|) \nabla_1 u(x) dx \geq \int_{\Omega} \gamma^N(|u(x)|) \nabla_1 u(x) dx \geq \int_0^{\infty} \gamma^N(t) \lambda(m_n A_t) dt.$$

Переходя к пределу при $N \rightarrow \infty$, получаем неравенство (3). ►

2. Интегральные неравенства

Функцию $\Phi: \mathbb{R}^n \rightarrow \mathbb{R}_+ \cup \{+\infty\}$ будем называть *функцией Юнга*, если функция Φ выпукла, четна на $\mathbb{R}^n$, $\Phi(\theta) = 0$ и при каждом $h > 0$ множество $\mathbb{P}(h) = \{p \in \mathbb{R}^n : \Phi(p) \leq h\}$ есть замкнутое ограниченное тело в $\mathbb{R}^n$. Функцию Юнга Φ назовём *изотропной*, если $\Phi(p) = \Phi_1(|p|)$, где Φ_1 – функция Юнга одного переменного.

Сопоставим функции Юнга Φ сопряженную к ней

$$\Phi^*(q) = \sup_{p \in \mathbb{R}^n} (\langle p, q \rangle - \Phi(p)),$$

где $\langle p, q \rangle$ – скалярное произведение в $\mathbb{R}^n$. Определяемая таким образом функция Φ^* есть функция Юнга на $\mathbb{R}^n$ [11].

Функцию $\Phi^\circ: \mathbb{R} \rightarrow \mathbb{R}_+ \cup \{+\infty\}$ будем называть *округлением* функции Юнга Φ , если функция $\Phi^\circ(r)$ четна на $\mathbb{R}$, $\Phi^\circ(0) = 0$, функция $r \rightarrow \Phi^\circ(r)$ непрерывна слева при $r \geq 0$ и нижние лебеговы множества $\{p : \Phi(p) \leq h\}$, $\{p : \Phi^\circ(|p|) \leq h\}$ функций Φ и $\Phi^\circ(|\cdot|)$ имеют одинаковую n -мерную меру при любом $h \geq 0$. Аналитическое определение функции Φ° эквивалентно следующему геометрическому факту: надграфик функции $\Phi^\circ(|p|)$ является симметризацией по Шварцу [12] надграфика функции $\Phi(p)$. Если функции $\Phi^\circ, \Phi^{*\circ}$ суть округления функций Юнга Φ и Φ^* соответственно,

$$\Phi^{*\circ}(r) = \sup_s (rs - \Phi^{*\circ}(s)), \quad (6)$$

то 1) $\Phi^\circ, \Phi^{*\circ}, \Phi^{*\circ*}$ – функции Юнга на $\mathbb{R}$; 2) существуют такие зависящие лишь от n положительные постоянные α_n, β_n , что для любой функции Юнга Φ справедливы оценки

$$\Phi^\circ(\alpha_n r) \leq \Phi^{*\circ*}(r) \leq \Phi^\circ(\beta_n r) \quad \forall r \in \mathbb{R}. \quad (7)$$

Доказательства оценок (7) и других свойств операции округления можно найти в [13]. Для изотропной функции Юнга Φ имеют место хорошо известные равенства $\Phi^{*\circ} = \Phi^{*\circ*}, \Phi^\circ = \Phi^{*\circ*}$ [11].

Функцию $f: \mathbb{R}_+ \times \mathbb{R}^n \rightarrow \mathbb{R} \cup \{+\infty\}$ назовём *интегрантом Юнга*, если 1) при любом $t \geq 0$ функция $f_t(p) = f(t, p)$ есть функция Юнга на $\mathbb{R}^n$; 2) функция $t \rightarrow f(t, p)$ измерима по Борелю при любом $p \in \mathbb{R}^n$. По определению $f^*(t, q) = f_t^*(q), f^\circ(t, r) =$

$f_t^\circ(r)$, т.е. введенные выше операции выпуклого анализа применяются к функции f_t . Если f – интегрант Юнга, то и f^*, f° также интегранты Юнга [14].

При любом $h \geq 0$ множество $\mathbb{Q}_t(h) = \{q \in \mathbb{R}^n : f_t^*(q) \leq h\}$ есть выпуклый центрально-симметричный компакт. Положим $k(p; t, h) = \max\{\langle p, q \rangle, q \in \mathbb{Q}_t(h)\}$. Таким образом, $k(p; t, h)$ есть опорная функция множества $\mathbb{Q}_t(h)$. Из определения функции $k(\cdot)$ вытекают неравенства

$$k(p; t, h) - h \leq f(t, p), \quad k(p; t, h) \leq \rho(t, h)|p|, \quad (8)$$

где $\rho(t, h) = \max\{|q|, q \in \mathbb{Q}_t(h)\}$. При возрастании h функция $k(p; t, h)$ не уменьшается. Для изотропного интегранта f сопряженный интегрант f^* также изотропен, поэтому $\mathbb{Q}_t(h) = \{q : |q| \leq \rho(t, h)\}$ и $k(p; t, h) = \rho(t, h)|p|$. Для любой вещественной B -измеримой на $\mathbb{R}_+$ функции $r(t)$ функция $t \rightarrow k(p; t, r(t))$ измерима по Борелю [14]. В частности, если f – изотропный интегрант, то B -измерима функция $\rho(t, r(t))$.

Пусть Ω ограниченная область в $\mathbb{R}^n$. Обозначим через $W(\Omega)$ совокупность почти везде конечных функций $u : \Omega \rightarrow \mathbb{R}$, для которых при любом $l > 0$ её срезка $u^l = \min\{|u|, l\} \operatorname{sgn}(u)$ по уровню l принадлежит $W_1^1(\Omega)$. Класс $W(\Omega)$ включает в себя пространство $W_1^1(\Omega)$. Перестановка $\bar{u}$ функции u из $W(\Omega)$ абсолютно непрерывна на каждом отрезке $[\delta, a]$ ($0 < \delta < a = m_n \Omega$) [4], [13]. Если $A_t = \{x \in \Omega : |u(x)| > t\}$ и $\mu(t) = m_n(A_t) = m_1\{s \in [0, a], \bar{u}(s) > t\}$ – функция распределения функции $u \in W(\Omega)$, то $t = \bar{u}(\mu(t)), s \geq \mu(\bar{u}(s))$, причём $s = \mu(\bar{u}(s))$, если функция $\mu(t)$ непрерывна в точке $t = \bar{u}(s)$. Если $u \in W(\Omega)$, $l > m > 0$, то $\nabla u^l(x) = \nabla u^m(x)$ при $x \in A_m$, поэтому почти всюду в Ω существует

$$\lim_{l \rightarrow \infty} \nabla u^l(x),$$

обозначаемый далее как $\nabla u(x)$.

Теорема 1. Пусть f – изотропный интегрант Юнга, f° – округление интегранта f , $\Omega \in J(\lambda)$, $a = m_n \Omega$, $u \in W(\Omega)$, $\bar{u}$ – перестановка функции u .

Тогда справедливо неравенство

$$\int_{\Omega} f(|u(x)|, \nabla u(x)) dx \geq \int_0^a f^\circ\left(\bar{u}(s), \frac{d\bar{u}}{ds}(s)\lambda(s)\right) ds. \quad (9)$$

◀ Пусть $u \in W(\Omega)$. Функция $p \rightarrow f(|u(x)|, p)$ почти для всех x из Ω выпукла, полунепрерывна снизу по p и конечна в некоторой окрестности θ , а при каждом p функция $f(|u(x)|, p)$ измерима по Лебегу. Отсюда следует, что функция $f(|u(x)|, \nabla u(x))$ измерима по Лебегу. Если эта функция не суммируема по Ω , то левая часть (9) считается равной $+\infty$. Аналогичное соглашение принимается и для правой части (9). Повторяя проведенные в [14] рассуждения, можно показать, что (9) достаточно установить для ограниченных и неотрицательных функций u .

Итак, не нарушая общности, считаем, что $u \in W(\Omega) \cap L^\infty(\Omega)$ и $u(x) \geq 0$. В этом случае функция $\bar{u}$ – абсолютно непрерывна на $[0, a]$, а функция $\frac{d\bar{u}}{ds}(s)\lambda(s)$ суммируема по отрезку $[0, a]$ [2], [4]. Далее $\mu(t)$ – функция распределения функции $u(\cdot)$. Функционалы $I_{f^\circ}, I_{f^{\circ*}}$, определенные на $L(0, a)$ и $L^\infty(0, a)$ равенствами

$$I_{f^\circ}(z) = \int_0^a f^\circ(\bar{u}(s), z(s)) ds, \quad I_{f^{\circ*}}(y) = \int_0^a f^{\circ*}(\bar{u}(s), y(s)) ds, \quad (10)$$

сопряжены друг другу относительно обычной двойственности между пространствами $L(0, a)$ и $L^\infty(0, a)$. Отсюда следует, что

$$\begin{aligned} & \int_0^a f^\circ \left(\bar{u}(s), \frac{d\bar{u}}{ds}(s) \lambda(s) \right) ds = I_{f^\circ} \left(\left| \frac{d\bar{u}}{ds} \right| \lambda \right) = \\ & = \sup_{y \in L^\infty(0, a)} \left\{ \int_0^a \left(\left| \frac{d\bar{u}}{ds}(s) \right| \lambda(s) y(s) - f^{\circ*}(\bar{u}(s), y(s)) \right) ds \right\}. \end{aligned} \quad (11)$$

В соотношении (11) *supremum* можно брать лишь по функциям y из $L^\infty(0, a)$, удовлетворяющим условиям:

- $i_1)$ $y(s) \geq 0$, $y(s) = 0$, если $\frac{d\bar{u}}{ds}(s) = 0$, $y(\cdot)$ измерима по Борелю;
- $i_2)$ функция $f^{\circ*}(\bar{u}(s), y(s))$ измерима по Борелю, конечна при всех s и суммируема по отрезку $[0, a]$.

Для доказательства (9) достаточно установить неравенство

$$\int_{\Omega} f(|u(x)|, \nabla u(x)) dx \geq \int_0^a \left(\left| \frac{d\bar{u}}{ds}(s) \right| \lambda(s) y(s) - f^{\circ*}(\bar{u}(s), y(s)) \right) ds \quad (12)$$

для каждой функции $y(\cdot)$, удовлетворяющей условиям $i_1), i_2)$. Фиксируем подобную функцию $y(\cdot)$ и определим функцию $r(t)$ на луче $\mathbb{R}_+$ равенством

$$r(t) = f^{\circ*}(\bar{u}(\mu(t)), y(\mu(t))) = f^{\circ*}(t, y(\mu(t))).$$

Функция $r(\cdot)$ измерима по Борелю, а функции $f^{\circ*}(\bar{u}(s), y(s))$ ($0 \leq s \leq a$) и $r(u(x))$ ($x \in \Omega$) равноизмеримы.

Пусть $k(p; t, h)$ есть опорная функция множества $\mathbb{Q}_t(h) = \{q \in \mathbb{R}^n : f_t^*(q) \leq h\}$. В силу изотропности интегранта f справедливо равенство $k(p; t, h) = \rho(t, h)|p|$, где $\rho(t, h) = \max\{|q|, q \in \mathbb{Q}_t(h)\}$. Функция $\gamma(t) = \rho(t, r(t))$ измерима по Борелю. Соотношение $Q(t, r(t)) = \{q : f^{\circ*}(t, |q|) \leq r(t) = f^{\circ*}(t, y(\mu(t)))\}$ влечёт за собой оценку $\gamma(t) \geq y(\mu(t))$. Из (8) вытекает неравенство

$$f(t, p) \geq \gamma(t)|p| - r(t) \geq y(\mu(t))|p| - r(t).$$

Его очевидным следствием является оценка

$$\int_{\Omega} f(u(x), \nabla u(x)) dx \geq \int_{\Omega} (y(\mu(u(x))) \nabla_1 u(x) - r(u(x))) dx. \quad (13)$$

Используя лемму 1 и замену переменных $t = \bar{u}(s)$, получаем последовательно

$$\int_{\Omega} y(\mu(u(x))) \nabla_1 u(x) dx \geq \int_0^\infty y(\mu(t)) \lambda(\mu(t)) dt = \int_0^a y(s) \left| \frac{d\bar{u}(s)}{ds} \right| \lambda(s) ds. \quad (14)$$

В силу равноизмеримости функций $f^{\circ*}(\bar{u}(s), y(s))$, $r(u(x))$ равны соответствующие интегралы

$$\int_{\Omega} r(u(x)) dx = \int_0^a f^{\circ*}(\bar{u}(s), y(s)) ds. \quad (15)$$

Объединение (13)–(15) влечет неравенства (12), (9). ►

В качестве приложения теоремы 1 рассмотрим многомерную вариационную задачу

$$g(u) = \int_{\Omega} G(x, u(x), \nabla u(x)) dx \rightarrow \inf,$$

$$u \geq 0, \quad u \in W_1^1(\Omega), \quad h(u) = \int_{\omega} H(u(x)) dx = 1.$$

Теорема 2. Пусть H – B -измеримая функция на $\mathbb{R}_+$, а функция $G(x, t, p)$ удовлетворяет неравенству $G(x, t, p) \geq f(t, p)$, где f – изотропный интегрант Юнга на $\mathbb{R}_+ \times \mathbb{R}^n$. Тогда значение рассматриваемой многомерной вариационной задачи не меньше значения следующей одномерной вариационной задачи:

$$\int_0^a f^{\circ} \left(z(s), \frac{dz}{ds}(s) \lambda(s) \right) ds \rightarrow \inf, \quad z(s) \geq 0, \quad \int_0^a H(z(s)) ds = 1,$$

где z – абсолютно непрерывные на каждом отрезке $[\delta, a]$ ($0 < \delta < a$) и убывающие на $(0, a]$ функции.

◄ Теорема 2 вытекает из теоремы 1. ►

Изопериметрическое условие $h(u) = 1$ можно заменить включением $u \in \mathfrak{M}$, где $\mathfrak{M}$ – перестановочно инвариантное множество: вместе с функцией u множество $\mathfrak{M}$ содержит все равноизмеримые с ней функции.

3. Симметризации функций и интегральные неравенства

Усиливая предположения относительно функции u , можно доказать аналог неравенства (9) для анизотропного интегранта Юнга f . Пусть $\overset{\circ}{W}_1^1(\Omega)$ – совокупность функций из $W_1^1(\Omega)$, обращающихся в нуль на границе области Ω . Последнее означает, что если функцию из $\overset{\circ}{W}_1^1(\Omega)$ продолжить на всё пространство $\mathbb{R}^n$, полагая её равной нулю на $\mathbb{R}^n \setminus \Omega$, то продолженная функция принадлежит $W_1^1(\mathbb{R}^n)$. Обозначим через $\overset{\circ}{W}$ совокупность неотрицательных почти везде конечных функций u на Ω , для которых при любом $l > 0$ функции $u^l = \min\{u, l\}$ принадлежат пространству $\overset{\circ}{W}_1^1(\Omega)$. Поскольку $\overset{\circ}{W}(\Omega) \subset W(\Omega)$, то определен градиент $\nabla u(x)$ функции u класса $\overset{\circ}{W}$. Перестановка $\bar{u}$ функции u из $\overset{\circ}{W}$ абсолютно непрерывна на каждом сегменте $[\delta, a]$ ($0 < \delta < a$) и $\bar{u}(a) = 0$.

Предложение 2. [14] Пусть f – интегрант Юнга на $\mathbb{R}_+ \times \mathbb{R}^n$, $u \in \overset{\circ}{W}(\Omega)$, $\bar{u}$ – перестановка u , $a_n = m_n\{p \in \mathbb{R}^n : |p| \leq 1\}$. Тогда справедливо неравенство

$$\int_{\Omega} f(u(x), \nabla u(x)) dx \geq \int_0^a f^{**} \left(\bar{u}(s), \frac{d\bar{u}(s)}{ds}(s) \lambda_0(s) \right) ds, \quad (16)$$

в котором функция f^{**} определена равенством (6), $\lambda_0(s) = n \sqrt[n]{a_n} s^{\frac{n-1}{n}}$.

Очевидна аналогия между неравенствами (9) и (16). Вместе с тем существенны и различия – интегрант f в предложении 2 может быть анизотропным, функция u в определенном смысле обращается в нуль на границе области Ω , функция $\lambda(s)$ заменена более простой функцией $\lambda_0(s)$. Для анизотропного интегранта f функции f° и f^{**} различны, однако из неравенств (7) следует их эквивалентность в том смысле, что $f^\circ(t, \bar{\alpha}_n r) \leq f^{**}(t, r) \leq f^\circ(t, \bar{\beta}_n r)$ и положительные постоянные $\bar{\alpha}_n, \bar{\beta}_n$ зависят только от n . Геометрическую основу предложения 2 составляет классическое неравенство Брунна–Минковского и вытекающая из него изопериметрическая теорема [12; гл. 5]. Отметим, что неравенства типа (16) верны и для функций u , обращающихся в 0 лишь на части границы области Ω . Соответствующие утверждения установлены в [15] для интегрантов f , четных по каждому из переменных p_i . Доказательства опираются на неравенство Лумиса–Уитни [12].

Соотношению (16) можно придать несколько иную форму. Функцию $u^\circ(x) = \bar{u}(a_n|x|^n)$ именуют симметризацией Шварца функции u . Эта функция определена на шаре $\Omega^\circ = \{x \in \mathbb{R}^n, |x| < R\}$, $(a_n R^n = m_n \Omega)$ и равноизмерима с функцией u . Справедливо включение $u^\circ \in \overset{\circ}{W}(\Omega^\circ)$ и верно равенство

$$\nabla_1 u^\circ(x) = \lambda_0(s) \left| \frac{d\bar{u}(s)}{ds}(s) \right|,$$

в котором $s = a_n|x|^n$. Поэтому (16) эквивалентно неравенству

$$\int_{\Omega} f(u(x), \nabla u(x)) dx \geq \int_{\Omega^\circ} f^{**}(u^\circ(x), \nabla_1 u^\circ(x)) dx. \quad (17)$$

Рассмотрим вариант (17), возникающий при замене симметризации по Шварцу симметризацией по Штейнеру. Напомним некоторые определения. Пусть $H = \{(x_1, \dots, x_{n-1}, x_n), x_n = 0\}$ – координатная гиперплоскость в $\mathbb{R}^n (n \geq 2)$, $P_H: \mathbb{R}^n \rightarrow H$ – оператор ортогонального проектирования, $l(x)$ – прямая, проходящая через точку x и ортогональная H , A – такое множество в $\mathbb{R}^n$, что для любого x из множества $P_H A$ пересечение $A \cap l(x)$ ограничено. Симметризацией Штейнера множества A относительно гиперплоскости H называется [12] множество

$$S_H A = \bigcup_{x \in P_H A} (A \cap l(x))^s,$$

где $(A \cap l(x))^s$ – принадлежащий $l(x)$ отрезок с центром в точке x , длина которого равна одномерной хаусдорфовой мере множества $A \cap l(x)$. При изучении симметризации Штейнера оказались полезными правила, относящиеся к операции Минковского [12]. В дальнейшем удобно точку $x = (x_1, \dots, x_{n-1}, x_n)$ из $\mathbb{R}^n$ записывать в виде (x', x_n) , где $x' = (x_1, \dots, x_{n-1}) \in \mathbb{R}^{n-1}$, так что $P_H x = (x', 0)$.

Введем понятие *симметризации по Штейнеру* функции Юнга $\Phi(p)$ ($p \in \mathbb{R}^n$). Надграфик $\text{epi}\Phi$ функции Φ есть выпуклое замкнутое подмножество $\mathbb{R}^n \times \mathbb{R}$. Симметризация $\text{epi}\Phi$ относительно гиперплоскости $H \times \mathbb{R} \subset \mathbb{R}^n \times \mathbb{R}$ совпадает с надграфиком некоторой функции, называемой симметризацией Φ относительно H в возрастающем порядке и обозначаемой символом Φ^S . Из определения функции Φ^S вытекает равенство $\{p \in \mathbb{R}^n : \Phi^S(p) \leq h\} = S_h\{p \in \mathbb{R}^n : \Phi(p) \leq h\}$ – нижние лебеговы множества функции Φ^S совпадают с симметризациями по Штейнеру нижних лебеговых множеств функции Φ .

Перейдем к определению симметризации по Штейнеру суммируемых функций. Пусть u – неотрицательная функция из $L(\Omega)$. Её подграфик (ординатное множество) $\text{ordu} = \{(x, t) \in \mathbb{R}^n \times \mathbb{R} : x \in \Omega, 0 \leq t \leq u(x)\}$ есть подмножество $\mathbb{R}^n \times \mathbb{R}$, пересечение которого с каждой прямой, проходящей через точку (x', t) , $x' \in H, t > 0$, и перпендикулярной $H \times \mathbb{R}$, есть ограниченное множество. Поэтому определена симметризация по Штейнеру множества $\text{ordu} \subset \mathbb{R}^n \times \mathbb{R}$ относительно гиперплоскости $H \times \mathbb{R} \subset \mathbb{R}^n \times \mathbb{R}$. Результат этой симметризации есть множество $S_H(\text{ordu}) \subset \mathbb{R}^n \times \mathbb{R}$. Оно совпадает с подграфиком некоторой неотрицательной функции u^c , суммируемой на множестве $\Omega^c = S_H\Omega$ и называемой симметризацией по Штейнеру функции u относительно H в убывающем порядке. Почти при всех $x' \in P_H\Omega$ функция $u^c(x', \cdot)$ совпадает с перестановкой функции $u(x', \dots)$ в симметрично убывающем порядке ([3], с. 309). Это свойство может быть положено в основу определения функции u^c .

Если u – неотрицательная функция из $\overset{\circ}{W}_1^1(\Omega)$, то $u^c \in \overset{\circ}{W}_1^1(\Omega^c)$. Автором получены широкие обобщения этого факта. Например, установлено [16], [17], что для любой функции Юнга $\Phi: \mathbb{R}^n \rightarrow \mathbb{R} \cup \{+\infty\}$ и любой функции u класса $\overset{\circ}{W}(\Omega)$ имеет место неравенство

$$\int_{\Omega} \Phi(\nabla u(x)) dx \geq \int_{\Omega^c} \Phi^{*S*}(\nabla u^c(x)) dx. \quad (18)$$

Вариант неравенства (18) верен и для интегранта Юнга.

Теорема 3. Пусть f – интегрант Юнга на $\mathbb{R}_+ \times \mathbb{R}^n$, $u \in \overset{\circ}{W}(\Omega)$. Тогда справедливо неравенство

$$\int_{\Omega} f(u(x), \nabla u(x)) dx \geq \int_{\Omega^c} f^{*S*}(u^c(x), \nabla u^c(x)) dx. \quad (19)$$

◀ Доказательство аналогично доказательству теоремы 1, поэтому ограничимся указанием его схемы. Вначале устанавливается вариант леммы 1. Соответствующее утверждение составляет содержание леммы 3 из [17], относящейся к так называемым простым (полиэдральным) функциям u и интегрантам f , сублинейным по переменному p . Неравенство (4) этой работы может быть с помощью подходящего предельного перехода распространено на функции u класса $\overset{\circ}{W}(\Omega)$; условие сублинейности f по переменной p при этом ещё сохраняется. От требования сублинейности f по переменной p можно отказаться, используя двойственность выпуклых функционалов $I_{f^{*S*}}, I_{f^{*S}}$, определяемых на пространствах $L(\Omega^c)$, $L^\infty(\Omega^c)$ аналогич-

ными (10) равенствами

$$I_{f^{*S^{*}}}(z) = \int_{\Omega^c} f^{*S^{*}}(u^c(x), z(x)) dx, \quad I_{f^{*S}}(y) = \int_{\Omega^c} f^{*S}(u^c(x), y(x)) dx,$$

Эта двойственность позволяет вывести неравенство (19) из более простого соотношения

$$\int_{\Omega} f(u(x), \nabla u(x)) dx \geq \int_{\Omega^c} (\langle \nabla u^c(x), y(x) \rangle - f^{*S}(u^c(x), y(x))) dx. \quad (20)$$

Неравенство (20) аналогично неравенству (12). И в этом случае для доказательства (19) достаточно проверить (20) не для всех функций y из $L^{\infty}(\Omega^c)$, а лишь для функций, удовлетворяющих условиям типа i_1, i_2). ►

Основное отличие теоремы 3 от известных принципов симметризации (см., например, [1] – [10]) связано с анизотропностью интегранта f . Теорема 3 очевидным образом переносится на симметризации относительно произвольной однородной гиперплоскости H . Как известно, симметризация относительно любого пространства $V \subset \mathbb{R}^n$ может быть получена как результат последовательного применения симметризации Штейнера относительно бесконечной системы гиперплоскостей [12]. В частности, таким образом могут быть получены аналоги теоремы 3 для k -мерной симметризации по Штейнеру.

Список литературы / References

- [1] Polya G., Szego G., *Isoperimetric Inequalities in Mathematical Physics*, Princeton, 1951.
- [2] Мазья В.Г., *Пространства С.Л. Соболева*, Изд-во Ленингр. ун-та, Ленинград, 1985; English transl.: Maz'ja Vladimir G., *Sobolev spaces*, Translated from the Russian by T.O. Shaposhnikova, Springer Series in Soviet Mathematics, Springer-Verlag, Berlin, 1985.
- [3] Соболев С.Л., *Введение в теорию кубатурных формул*, Наука, М., 1974; [Sobolev S. L., *Introduction to the Theory of Cubature formulas*, Nauka, Moscow, 1974, (in Russian).]
- [4] Коляда В.И., “Перестановки функций и теоремы вложения”, *УМН*, **44**:5 (1989), 61–95; English transl.: Kolyada V.I., “Rearrangements of functions and embedding theorems”, *Russian Math. Surveys*, **44**:5 (1989), 73–117.
- [5] Evans L.S. and Gariepy R.F., *Measure theory and fine properties of functions*, CRC Press, Boca Raton, Florida, 1992.
- [6] Kawohl B., *Rearrangements and convexity of level sets in P.D.E.*, Lectures Notes in Math., **1150**, Springer-Verlag, Berlin, 1985.
- [7] Talenti G., “On Isoperimetric Theorems of Mathematical Physics”, *Handbook of convex Geometry*, **B**, Amsterdam, New York, North-Holland, 1993.
- [8] Kesavan S., *Symmetrization & Applications*, World Scientific, New Jersey, 2006, 160 с.
- [9] Rakotoson J.-M., *Rearrangement Relatif: Un instrument destimations dans les problemes aux limites*, Mathematiques et Applications (French Edition), **64**, Springer, 2008.
- [10] Solynin A. Yu., “Continuous symmetrization via polarization”, *Algebra i Analis*, **24**:1 (2012), 157–222.
- [11] Rockafellar R.T., *Convex Analysis*, Princeton University Press, Princeton, New Jersey, 1970.
- [12] Hadwiger H., *Vorlesungen über Inhalt, Oberfläche und Isoperimetrie*, **1150**, Springer-Verlag, 1957.

- [13] Климов В.С., “Теоремы вложения и геометрические неравенства”, *Изв. АН СССР. Сер. матем.*, **40**:3 (1976), 645–671; English transl.: Klimov V.S., “Imbedding theorems and geometric inequalities”, *Mathematics of the USSR–Izvestiya*, **10**:3 (1976), 615–638.
- [14] Климов В.С., “Об оценках снизу некоторых интегральных функционалов”, *Качественные и приближенные методы исследования операторных уравнений*, Ярослав. гос. ун-т, Ярославль, 1981, 77–87; [Klimov V. S., “Ob ocenках snisu nekotoryh integralnyh funkcionalov”, *Kachestvennye i priblizhennye metody issledovaniya operatornyh uravnenii*, Yar. gos. un-t, Yaroslavl, 1981, 77–87, (in Russian).]
- [15] Климов В.С., “К теоремам вложения анизотропных классов функций”, *Матем. сб.*, **127(169)**:2(6) (1985), 198–208; English transl.: Klimov V.S., “On imbedding theorems for anisotropic classes of functions”, *Mathematics of the USSR–Sbornik*, **55**:1 (1986), 195–205.
- [16] Климов В.С., “О симметризации анизотропных интегральных функционалов”, *Известия ВУЗов. Математика*, 1999, № 8, 26–32; English transl.: Klimov V. S., “On the symmetrization of anisotropic integral functionals”, *Russian Mathematics (Izvestiya VUZ. Matematika)*, **43**:8 (1999), 23–29.
- [17] Климов В.С., “Симметризация функций из пространств Соболева”, *Известия ВУЗов. Математика*, 2002, № 11, 45–51; English transl.: [Klimov V. S., “Symmetrization of functions from Sobolev spaces”, *Russian Mathematics (Izvestiya VUZ. Matematika)*, **46**:11 (2002), 41–47.

Klimov V. S., "Isoperimetric and Functional Inequalities", *Modeling and Analysis of Information Systems*, **25**:3 (2018), 331–342.

DOI: 10.18255/1818-1015-2018-3-331-342

Abstract. We establish lower estimates for an integral functional

$$\int_{\Omega} f(u(x), \nabla u(x)) dx,$$

where Ω – a bounded domain in $\mathbb{R}^n$ ($n \geq 2$), an integrand $f(t, p)$ ($t \in [0, \infty)$, $p \in \mathbb{R}^n$) – a function that is B -measurable with respect to a variable t and is convex and even in the variable p , $\nabla u(x)$ – a gradient (in the sense of Sobolev) of the function $u: \Omega \rightarrow \mathbb{R}$. In the first and the second sections we utilize properties of permutations of differentiable functions and an isoperimetric inequality $H^{n-1}(\partial A) \geq \lambda(m_n A)$, that connects $(n-1)$ -dimensional Hausdorff measure $H^{n-1}(\partial A)$ of relative boundary ∂A of the set $A \subset \Omega$ with its n -dimensional Lebesgue measure $m_n A$. The integrand f is assumed to be isotropic, i.e. $f(t, p) = f(t, q)$ if $|p| = |q|$. Applications of the established results to multidimensional variational problems are outlined. For functions u that vanish on the boundary of the domain Ω , the assumption of the isotropy of the integrand f can be omitted. In this case, an important role is played by the Steiner and Schwartz symmetrization operations of the integrand f and of the function u . The corresponding variants of the lower estimates are discussed in the third section. What is fundamentally new here is that the symmetrization operation is applied not only to the function u , but also to the integrand f . The geometric basis of the results of the third section is the Brunn-Minkowski inequality, as well as the symmetrization properties of the algebraic sum of sets.

Keywords: permutation, convex function, measure, gradient, symmetrization, isoperimetric inequality

On the authors:

Vladimir S. Klimov, orcid.org/0000-0001-9560-8315, Doctor of Science, P.G. Demidov Yaroslavl State University, 14 Sovetskaya str., Yaroslavl, 150003, Russian Federation, e-mail: VSK76@list.ru