МНШ 2022 – отчет

Корешков Василий Романович, математик, лаб. 11, 13.06.1999

### **Объявленные цели проекта**

В проекте изучались C(6)-T(3)-группы и двухкомпонентные ресурсные сети. Были поставлены следующие задачи:

* Исследовать свойства двухкомпонентных ресурсных сетей;
* Изучить метод групповых диаграмм, проанализировать имеющиеся применения метода для решения задач вхождения в подгруппу;
* Для произвольной группы C(6)-T(3), которая не содержит элементов конечного порядка, построить свободную подгруппу ранга 2 и указать алгоритм, решающий проблему вхождения в построенную подгруппу;
* Найти применение полученных для C(6)-T(3)-групп результатов в криптографии.

### **Степень выполнения поставленных в проекте задач**

* Двухкомпонентные ресурсные сети были исследованы, а именно, были сформулированы теоремы, описывающие поведение двухкомпонентных ресурсных сетей во времени, в том числе и их асимптотические свойства;
* Метод групповых диаграмм был изучен в достаточной степени, равно как и применения этого метода для решения задач комбинаторной теории групп, в частности, задачи вхождения в подгруппу;
* Свободная подгруппа ранга 2 группы класса C(6)-T(3), не содержащей элементов конечного порядка, была построена и был получен алгоритм, решающий проблему вхождения в построенную подгруппу;
* Были исследованы возможные применения полученных для C(6)-T(3)-групп результатов в криптографии.

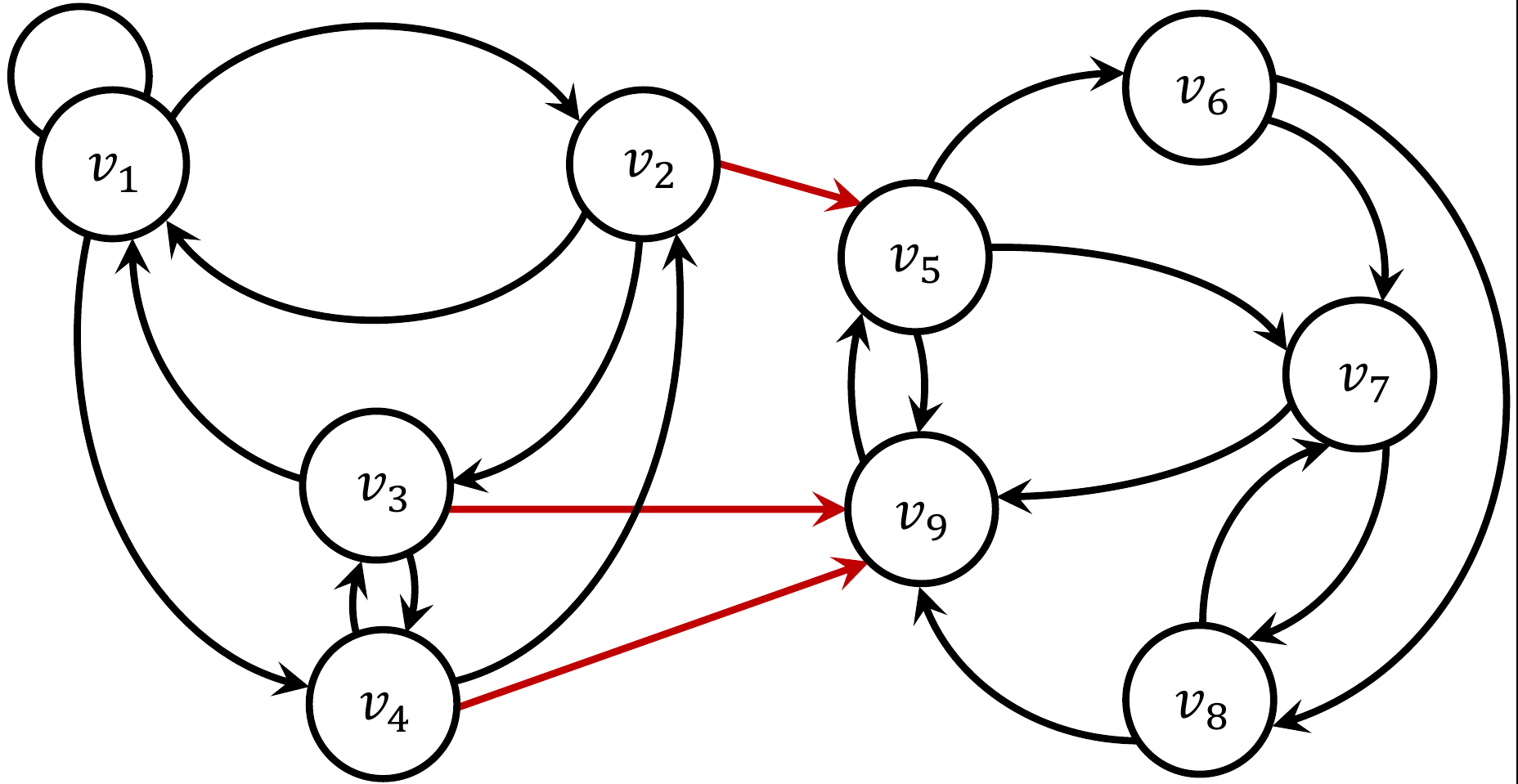
### **Полученные за отчетный год важнейшие результаты**

Работу можно разделить на две части: исследование двухкомпонентных ресурсных сетей и C(6)-T(3)-групп. Данные части объединены возможностью представить обе модели сетевом виде, т.е. в виде графа. Полученные для каждой части результаты приведены ниже.

##### Двухкомпонентные ресурсные сети

Ресурсная сеть представляет собой нелинейную модель потока, работающую в дискретном времени. Вершины сети синхронно перераспределяют некоторый бесконечно делимый ресурс. На каждом временном шаге каждая вершина отправляет ресурс всем своим соседям по одному из двух правил с пороговым переключением. Выбор правила зависит от количества ресурса в вершине. Если ресурс в вершине больше, чем общая пропускная способность ее исходящих ребер, он отправляет полную пропускную способность каждому ребру (в этом случае говорят, что вершина работает по правилу 1); в противном случае вершина отдает весь ресурс, распределяя его пропорционально пропускной способности исходящих ребер (в этом случае говорят, что вершина работает по правилу 2). Вершины имеют неограниченные емкости. Подробнее о модели можно прочитать в [2]. Там же вводятся понятия матрицы пропускной способности , стохастической матрицы , состояния сети , предельного состояния сети , общего ресурса сети , пороговое значение общего ресурса , вершины-аттрактора.

Двухкомпонентные ресурсные сети являются частным случаем общей модели ресурсной сети. Двухкомпонентные ресурсные сети представляют собой ресурсную сеть с двумя сильно связанными компонентами, т.е. такую сеть, в которой есть только ребра от первой сильно связной компоненты (называемой *переходной* компонентой с вершинами) до второй (называемой *финальной*, с вершин). Пусть n — общее количество вершин в сети (Рис.1.1).



*Рисунок 1.1 — Двухкомпонентная ресурсная сеть. Вершины ( - ) принадлежат переходной составляющей; вершины ( - ) образуют финальную компоненту;*

*.*

Были получены следующие результаты:

**Теорема 1.1.** *Существует конечный момент времени такой, что при все вершины переходной компоненты работают по правилу 2.*

Теорема 1.1 утверждает, что исследование всякого возможно распределения ресурса в переходной компоненте рано или поздно сводится к линейному случаю. Следующая теорема показывает, как ведет себя сеть в линейном случае.

**Теорема 1.2.** *Если вся двухкомпонентная сеть целиком работает по правилу 2, то общее количество ресурса в переходной компоненте стремится к нулю при стремлении времени к бесконечности.*

**Теорема 1.3.** *В двухкомпонентной ресурсной сети при любом значении и начальном распределении общего ресурса общее количество ресурса в переходной компоненте стремится к нулю при стремлении времени к бесконечности.*

Предположим, что финальная компонента ресурсной сети является регулярной. Пусть T будет пороговым значением общего ресурса для финальной компоненты. Пусть сеть задана матрицей:

**Теорема 1.4**. *Если , то существует единственное предельное состояние, не зависящее ни от начального распределения полного ресурса , ни от блоков и матрицы емкости .*

**Теорема 1.5**. *Если , то для любого начального состояния существует предельное состояние . Если, кроме того, финальная компонента содержит только один аттрактор, то это предельное состояние зависит только от W, т. е. не зависит ни от начального распределения полного ресурса, ни от блоков и матрицы емкости .*

Следующая теорема устанавливает связь модели двухкомпонентной ресурсной сети с неоднородными цепями Маркова в явном виде:

**Теорема 1.6**. *Для двухкомпонентной ресурсной сети, если , то для любого начального состояния неоднородная цепь Маркова со стохастическими матрицами сильно эргодична.*

##### –группы без кручения

Пусть группа задана своим копредставлением. А именно, , где — конечное множество символов, — свободная группа с образующими из , то есть множество всех слов в символах из , дополненное множеством обратных слов, образующее группу относительно операции конкатенации, а — конечное множество определяющих соотношений, то есть конечное подмножество . Тогда суть факторгруппа группы по нормальному замыканию множества в : . Таким образом, группа представляет собой не множество слов, а множество классов эквивалентности слов. Проблема равенства слов состоит в том, чтобы по двум словам из понять, принадлежат ли они одному классу эквивалентности в или нет. Проблема вхождения в подгруппу состоит в том, чтобы по заданному слову и подгруппе определить, принадлежит ли слово некоторому классу эквивалентности, являющемуся элементом указанной подгруппы.

В рассматриваемом классе групп () проблема равенства слов разрешима за квадратичное относительно длины слова время [5]. Проблема вхождения в подгруппу, в общем случае, оказывается неразрешимой [6]. В работе же рассматривается подкласс групп таких групп, а именно группы, не содержащие элементов конечного порядка, т.е. группы без кручения.

В работе используется метод групповых диаграмм — диаграмм Ван Кампена. Формально *диаграммой Ван Кампена над группой*  называется планарный конечный клеточный 2-комплекс , обладающий следующими свойствами [6]:

1. связен и односвязен;
2. Каждому ребру сопоставляется ориентация и метка из ;
3. Для каждой области (2-клетки) произведение меток ее границы суть точно некоторое слово из , либо его обращение, либо его циклическая перестановка.

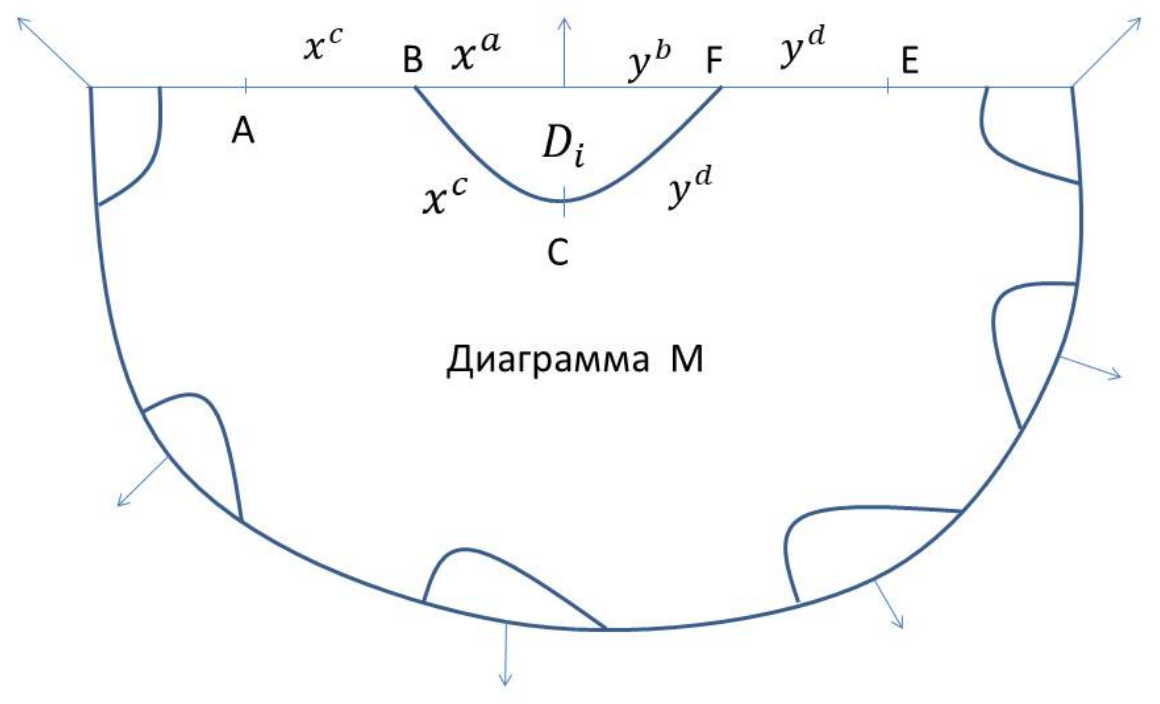


Рисунок 2.1 — Пример диаграммы Ван Кампена

Пример такой диаграммы показан на Рисунок 2.1 —. Таким образом, диаграммы Ван Кампена представляют собой специальные сетевые модели, сопоставляемые в соответствие данной группе. С помощью данных моделей удается доказывать нетривиальные факты о группах.

В ходе работы была сформулирована и доказана следующая основная теорема:

**Теорема 2.1.** *Пусть — -группа без кручения. Обозначим через n максимальную длину слова из . Тогда любая подгруппа , порожденная степенями некоммутирующих образующих бесконечного порядка, свободна.*

Стоит отметить, что данная теорема является обобщением так называемой «леммы о пинг-понге» для гиперболических групп [7]:

**Теорема 2.2.** *Пусть — гиперболическая группа без кручения. Пусть — два некомутирующих образующих из . Тогда существует подгруппа — свободна.*

Доказательство данной теоремы проходит от противного и доказывается, что если некоторое слово вида равно единице в группе , то после проведения всех свободных сокращений в нем оно оказывается пустым. Это и означает, что подгруппа свободная.

Доказательство основывается на понятии –сокращения и –сокращения, которые представляют собой специфические преобразования диаграммы Ван Кампена для некоторого слова. Использовались факты, известные из теории малых сокращений (раздел комбинаторной теории групп, занимающийся диаграммами Ван Кампена), например лемма Ван Кампена [8], лемма об обязательном наличии – и –сокращений в единичном слове [9], а также общие сведения из теории групп.

Подгруппа, построенная данным образом, примечательна тем, что для нее разрешима проблема вхождения:

**Теорема 2.3.** *Пусть — -группа без кручения, n — максимальная длина слова из , — подгруппа из теоремы 1. В таком случае, проблема вхождения в эту группу разрешима, а именно, существует конечный (т.е. терминирующий за конечное время) алгоритм, определяющий по произвольному данному слову , принадлежит ли это слово или нет.*

Для доказательства теоремы используется следующий факт [10]:

**Предложение 2.1**. *Пусть — -группа без кручения. Тогда существуют такие константы , что для любых равных в слов и выполнятся , где — длина слова (количество букв в слове).*

Иначе говоря, равные в группе слова имеют не сильно отличающиеся длины. Алгоритм состоит в том, чтобы перебрать все слова, записанные в виде , по возрастанию длины и сравнить с данным . Таких слов будет, ввиду последнего предложения, конечное множество.

Теорема 2.3 обобщается для более широкого класса подгрупп. Точнее, верно следующее:

**Следствие 2.1.** *Пусть — -группа без кручения. Пусть — произвольная подгруппа такая, что существует алгоритм, который по заданному числу выдает все слова-представители классов эквивалентности , у которых длина не больше . В таком случае проблема вхождения в разрешима.*

Была получена оценка времени работы алгоритма.

**Следствие 2.2.** *Указанный в теореме 2 алгоритм терминирует не более чем за экспоненциальное время, а точнее, при фиксированной группе и подгруппе существует такая константа , что для произвольного слова время работы алгоритма ограничивается величиной .*

Несмотря на то, что данный алгоритм выполняется долго, в ходе экспериментов выявлено, что довольно часто время работы алгоритма можно сократить за счет того, что после проведения в слове всех – и –сокращений оказывается, что получившееся слово есть в точности слово для некоторых . Данное соображение позволяет использовать указанную подгруппу в криптографических алгоритмах, например в протоколе обмена ключами Аншела-Аншела-Голдфелда в качестве платформенной группы [11]. Следующие соображения говорят в пользу использования : группа — свободная ранга 2, поэтому слова, записанные в элементах этой группы, никак не ограничиваются; в данной группе легко разрешима проблема равенства.

Возможно и иное применение полученных результатов. В [12] было сформулировано понятие – и –удлинений — операций, обратных к – и –сокращениям. Обозначим действие нескольких – и –удлинений на слово за , а последовательное действие всевозможных – и –сокращений за . Суть в том, что для произвольного слова не равно, в общем случае, побуквенно слову (хотя и равно ему в группе). Однако если , то наверняка равно побуквенно. Таким образом, — преобразование, оставляющее на месте все слова из , но, в общем случае, меняющее все остальные слова.

### **Степень новизны полученных результатов и сопоставление полученных результатов с мировым уровнем**

##### Двухкомпонентные ресурсные сети

Ресурсная сеть была впервые предложена в [1]. С тех пор возникла теория ресурсных сетей, их краткое описание можно найти в [2]. В этой статье также описываются две двухпороговые модификации стандартной модели. Некоторые другие модели, основанные на стандартной ресурсной сети, были разработаны другими исследовательскими группами [3] [4].

##### –группы без кручения

Работа была связана с двумя пересекающимися направлениями исследований в мировой науке.

С одной стороны, проводятся исследования в рамках теории малых сокращений. Каноническими трудами по теории малых сокращений являются [8] [6] [5]. На данный момент активно ведутся попытки обобщить теорию малых сокращений на гиперболические группы [7] [13] [14] [15] и группы Бернсайда [16] [17]. Интересные результаты получены при исследовании частоты встречаемости групп с малыми сокращениями [18]. Группам с неметрическими условиями () посвящены работы [9] [19] [20] [13].

С другой стороны, мировым сообществом ведется активный поиск эффективных и безопасных криптографических алгоритмов, основанных на теории групп. Подробную информацию о многообразии предлагаемых подходов можно получить из большого количества обзорных исследований, например [21] [22] [23]. Большинство подходов основано на использовании тех или иных «проблем» теории групп: проблема равенства, проблема поиска сопряженного элемента, проблема проверки сопряженности, проблема вхождения в подгруппу [24], проблема факторизации, проблема декомпозиции и многие другие. Предпринимались попытки представить в качестве платформенной группы свободные группы, о чем можно подробнее прочитать в [21].

Особого внимания заслуживают работы, в которых группы с условиями малых сокращений использовались в криптографии. Во-первых, это работа [12], в которой в качестве платформенной группы была выбрана группа с условиями , а также представлен специальный алгоритм, работающий именно с такими группами. Во-вторых, это работа [25], в которой была представлена модификация схемы Шамира, которая должна работать с группами.

Насколько известно автору, до настоящего момента попыток использовать в качестве платформенной группы –группы не предпринималось.

### **Список литературы**

1. Kuznetsov, O.P. Uniform Resource Networks. I. Complete Graphs. Autom. Remote. Control. 2009, 70, 1767–1775.
2. Zhilyakova, L. Single-Threshold Model Resource Network and Its Double-Threshold Modifications. Mathematics 2021, 9, 1444.
3. Skorokhodov, V.A.; Sviridkin, D.O. Regular periodic dynamic resource networks. Itogi Nauk. Tekhniki. Seriya Sovrem. Mat. Prilozheniya. Temat. Obz. 2021, 192, 117–124.
4. Antonova, V.M.; Zakhir, B.M.; Kuznetsov, N.A. Modeling of Graphs with Different Types of Reachability in Python. J. Commun. Technol. Electron. 2019, 64, 1464–1472.
5. Магнус Д., Каррас А., Солитер Д. Комбинаторная теория групп. — М. : Наука, 1974. — С. 1—456. — Пер. с англ.
6. Ольшанский А. Ю. Геометрия определяющих соотношений в груп- пах. — М. : Наука, 1989. — С. 1—448. — (Современная алгебра).
7. Gromov M. Hyperbolic groups // Essays in Group Theory / под ред. M. L. Green. — Germany : Springer New York, 1987. — Гл. 8.2. С. 75—265. — ISBN 0-387-96618-8.
8. Линдон Р., Шупп П. Комбинаторная теория групп. — М. : Мир, 1980. — С. 1—447. — Пер. с англ.
9. Безверхний В. Н. О нормализаторах элементов в C(p)-T(q)-группах. // Алгоритмические проблемы теории групп и полугрупп. Межвузовский сборник научных трудов. Изд-во Тул. гос. пед. ун-та им. Л.Н.Толстого. — 1994. — С. 4—58.
10. Bezverkhnij N. V. On the solvability of the general word problem for a cyclic subgroup of a group with condition C(6) // Fundam. Prikl. Mat. — 1999. — Т. 5, № 1. — С. 39—46. — ISSN 1560-5159. — URL: mech.math. msu.su/~fpm/eng/99/991/99102h.htm.
11. Anshel I., Anshel M., Goldfeld D. An algebraic method for public-key cryptography // Mathematical Research Letters. — 1999. — Т. 6, № 3. — С. 287—291. — DOI: 10.4310/mrl.1999.v6.n3.a3.
12. Bezverkhniy N. V., Nikitina M. V. Asymmetric Secret Key Transfer Scheme over an Open Channel in K-Deterministic Groups with the Conditions C (3)–T (6) // Mathematics and Mathematical Modeling. — 2019. — Янв. — № 6. — С. 88—111. — DOI: 10.24108/mathm.0618.0000151.
13. Gruber D. Groups with graphical C(6) and C(7) small cancellation presentations // Transactions of the American Mathematical Society. — 2014. — Июль. — Т. 367, № 3. — С. 2051—2078. — DOI: 10 . 1090 / s0002 - 9947 - 2014 - 06198-9.
14. Hull M. Small cancellation in acylindrically hyperbolic groups // Groups, Geometry, and Dynamics. — 2016. — Т. 10, № 4. — С. 1077—1119. — DOI: 10.4171/ggd/377. — URL: <https://arxiv.org/abs/1308.4345.>
15. Bigdely H. Subgroup theorems in relatively hyperbolic groups and small- cancellation theory : дис. . . . канд. / Bigdely Hadi. — McGill University, 2013. — URL: https : / / escholarship . mcgill . ca / concern / theses / 4j03d3299.
16. Coulon R. Small cancellation theory and Burnside problem // Internat. J. Algebra Comput. 24 (2014), no. 3, 251-345. — 2013. — 27 февр. — Т. 24, № 03. — С. 251—345. — DOI: 10.1142/s0218196714500143. — arXiv: 1302.6933 [math.GR].
17. Coulon R., Gruber D. Small cancellation theory over Burnside groups // Advances in Mathematics. — 2019. — Сент. — Т. 353. — С. 722—775. — DOI: 10.1016/j.aim.2019.05.029.
18. Bishop A., Ferov M. Density of Metric Small Cancellation in Finitely Presented Groups // journal of Groups, complexity, cryptology. — 2020. — Сент. — Т. Volume 12, Issue 2. — DOI: 10.46298/jgcc.2020.12.2.6200.
19. Безверхний Н. В. Нормальные формы для элементов бесконечного порядка в группах с условиями C(3)-T(6) // Известия ТулГУ. Естественные науки. — 2010. — № 1. — С. 6—25.
20. Безверхний Н. В. Кольцевые диаграммы с периодическими метками и проблема степенной сопряжённости в группах с условиями C(3)- T(6) // Научное издание МГТУ им. Н.Э.Баумана. — 2014. — Т. No11. — С. 238—256.
21. Aspects of Nonabelian Group Based Cryptography: A Survey and Open Problems / B. Fine [и др.] // arXiv.org, e-Print Archive Mathematics. — 2011. — DOI: 10.48550/ARXIV.1103.4093. — URL: https://arxiv.org/abs/1103.4093v2 (дата обр. 06.04.2023).
22. Shpilrain V. Problems in group theory motivated by cryptography // arXiv.org, e-Print Archive Mathematics. — 2018. — DOI: 10 . 48550 / ARXIV.1802.07300. — URL: https://arxiv.org/abs/1802.07300v2 (дата обр. 28.03.2023).
23. Hasapis S. D., Panagopoulos D., Raptis E. A Survey of Group-based Cryptography // Journal of Applied Mathematics & Bioinformatics. — 2015. — Т. 5, № 3. — С. 73—96.
24. Shpilrain V., Zapata G. Using the subgroup membership search problem in public key cryptography. — 2006. — DOI: 10.1090/conm/418/07955. — URL: https://www.researchgate.net/publication/228626705\_Using\_the\_subgroup\_membership\_search\_problem\_in\_public\_key\_ cryptography (дата обр. 18.04.2023).
25. Habeeb M., Kahrobaei D., Shpilrain V. A Secret Sharing Scheme Based on Group Presentations and the Word Problem. — 2012. — Май. — DOI: 10.48550/ARXIV.1205.0157. — arXiv: 1205.0157 [cs.CR].

### **Методы и подходы, использованные в ходе выполнения проекта**

В работе использовался аппарат теории графов, теории цепей Маркова, теории матриц, линейной алгебры, теории групп, топологии, криптографии и комбинаторики. Основной инструмент — матрицы, цепи Маркова диаграммы Ван Кампена, понятия – и –сокращений.

### **Участие в научных мероприятиях и научных семинарах в 2022-2023 гг.**

### **Публикации**

* + [Жилякова Л.Ю., Корешков В.Р., Чаплинская Н.В. Some Properties of Stochastic Matrices and Non-Homogeneous Markov Chains Generated by Nonlinearities in the Resource Network Model // Mathematics. 2022. Vol.10, Iss. 21. С. 4095 (1-17).](https://www.ipu.ru/node/71157)
  + [Жилякова Л.Ю., Корешков В.Р. Graph Methods for Improving the Non-Optimal Solution of the Locomotive Assignment Problem under Time Constraints // Advances in Systems Science and Applications. 2022. Vol 22 No 2 (2022). С. 46-61 https://ijassa.ipu.ru/index.php/ijassa/article/view/1212.](https://www.ipu.ru/node/70900)

### **Краткая справка о научной деятельности**

Корешков Василий Романович

Email: [koreshkovhw@yandex.ru](mailto:koreshkovhw@yandex.ru)

С декабря 2021 года – математик лаборатории №11 «Интеллектуализации дискретных процессов и систем управления».