

ОТЗЫВ НАУЧНОГО РУКОВОДИТЕЛЯ
на диссертацию Царегородцева Кирилла Денисовича
«Правильные семейства функций и порождаемые ими
квазигруппы: комбинаторные и алгебраические свойства»,
представленную на соискание ученой степени
кандидата физико-математических наук
по специальности 1.1.5.

Математическая логика, алгебра, теория чисел и
дискретная математика
(физико-математические науки)

Конечные квазигруппы — перспективная платформа для реализации различных криптографических примитивов. В ряде практических криптоалгоритмов используются квазигруппы большого порядка, что исключает табличное задание. В качестве выхода из положения предлагается перейти от табличного задания к формульному. Одной из конструкций для формульного задания больших параметрических семейств квазигрупп являются правильные семейства функций, предложенные В. А. Носовым. Несмотря на существенные продвижения, в области правильных семейств остается открытым широкий спектр проблем: нахождение правильных семейств с компактным представлением и хорошими криптографическими свойствами, оценка мощности правильных семейств, как в общем случае, так и для отдельных классов, оценка мощности множества порождаемых квазигрупп, изучение свойств правильных семейств. В работе К. Д. Царегородцева получен ряд ярких результатов по этим вопросам, что обосновывает **актуальность и значимость** диссертационного исследования.

Работа К. Д. Царегородцева имеет следующую структуру. Во **введении** описываются цели работы, обосновывается актуальность и практическая значимость, приводятся основные результаты.

Первая глава содержит основные определения и обозначения, обзор известных результатов в области правильных семейств и крипто-

графических требований к квазигруппам (особенно отмечу отличный обзор по неассоциативности квазигрупп), а также включает в себя три новых результата: обобщение критерия правильности на случай, когда разные аргументы функций семейства могут принимать значения из разных множеств, новую конструкцию для порождения квазигрупп с помощью правильных семейств и новое квадратичное правильное семейство булевых функций.

Во **второй главе** изучаются критерии правильности семейства функций. Первая часть главы посвящена булевому случаю. Здесь автору удалось сделать яркую находку. Оказалось, что булевы правильные семейства находятся в естественном взаимно-однозначном соответствии с двумя известными математическими объектами: одностовыми ориентациями булева куба и булевыми сетями с наследственно единственной неподвижной точкой. Эта находка не только позволяет получить новые критерии правильности в терминах ориентации или неподвижных точек, но и дает возможность перевести известные результаты об ориентациях и булевых сетях на язык правильных семейств. Как следствие, возникают верхняя и нижняя оценка на число правильных семейств, утверждение о малости доли важного класса треугольных семейств, а также изящный критерий правильности в терминах запрета самодвойственных подсемейств. При переходе от булева случая к общему предлагаются новые большие классы правильных семейств — рекурсивно треугольных и локально треугольных. Завершает главу еще один любопытный критерий в терминах клик заданного размера в графе Келлера.

Третья глава посвящена новым свойствам правильных семейств. Здесь автор формулирует и доказывает теорему о стабилизаторе множества правильных семейств в общем случае, теорему о четности мощности полного прообраза любого элемента относительно действия правильного семейства в булевом случае, а также находит мощность образа двух важных квадратичных семейств булевых функций. Отмечу, что мощность образа семейства — важная характеристика, позволя-

ющая достаточно точно оценить мощность множества порождаемых квазигрупп. Завершает главу исследование алгебраических свойств отображений специального вида, заданных с помощью правильных семейств.

В **четвертой главе** исследуется ряд прикладных и алгоритмических задач. Предлагается новый квазигрупповой шифр, сохраняющий формат, основанный на квазигрупповых сдвигах. Описывается оптимизированный алгоритм проверки правильности булевых семейств. Излагаются результаты вычислительного эксперимента, оценивающего криптографические свойства квазигрупп, используемых в шифре, в частности, неассоциативность и полиномиальную полноту.

В **заключении** перечисляются основные результаты диссертации:

1. установлено естественное соответствие между правильными семействами булевых функций и одностокowymi ориентациями графов булевых кубов;
2. установлено естественное соответствие между правильными семействами булевых функций и булевыми сетями с наследственно единственной неподвижной точкой;
3. установлено естественное соответствие между правильными семействами в логике произвольной значности и кликами в обобщенных графах Келлера;
4. доказано, что стабилизатором множества правильных семейств функций являются изометрии пространства Хэмминга;
5. показано, что отображения, задаваемые с помощью правильных семейств булевых функций, всегда имеют четное число неподвижных точек;
6. получена оценка на число правильных семейств булевых функций, предложены оценки доли треугольных семейств среди всех правильных семейств булевых функций;

7. обнаружены и исследованы новые классы правильных семейств функций (рекурсивно треугольные, локально треугольные, сильно квадратичное семейство);
8. получены оценки на число рекурсивно треугольных семейств;
9. для двух важных правильных семейств булевых функций получены точные значения мощности образа;
10. предложен новый способ порождения квазигрупп на основе правильных семейств функций;
11. доказан ряд утверждений о числе ассоциативных троек в порождаемых квазигруппах;
12. предложен новый алгоритм шифрования, сохраняющего формат, основанный на квазигрупповых операциях.

Учитывая изложенное выше, можно утверждать, что содержание диссертации **свидетельствует** о том, что полученные в ходе ее создания **результаты являются новыми и вносят существенный вклад в решение научной задачи изучения свойств конечных квазигрупп в контексте криптографических приложений.**

Практическая значимость полученных результатов состоит, во-первых, в построении новых классов правильных семейств, которые могут быть использованы для построения квазигрупповых криптоалгоритмов; во-вторых, в новом квазигрупповом алгоритме симметричного шифрования, сохраняющего формат.

Основные результаты диссертации отражены в 9 статьях в рецензируемых журналах, в том числе 8 статьях в изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 1.1.5, а также докладывались на международных конференциях, в частности, X и XI симпозиуме «Современные тенденции в криптографии» (2021 и 2022 год), 11-й Международной конференции «Дискретные модели в теории управляющих систем» (2023

год), Третьей Международной конференции «Mathematics in Armenia: advances and perspectives» (2023 год), Международной конференции «Алгебра и математическая логика: теория и приложения» (2024 год), XX Международной научной конференции «Проблемы теоретической кибернетики» (2024 год), и на различных семинарах в МГУ имени М.В.Ломоносова, в частности, научно-исследовательском семинаре по алгебре механико-математического факультета МГУ под руководством Д. О. Орлова, М. В. Зайцева (2023 год), семинаре «Компьютерная алгебра» факультета ВМК МГУ и ВЦ РАН под руководством С. А. Абрамова (2023 год), семинаре «Теория автоматов» механико-математического факультета МГУ под руководством Э.Э. Гасанова (2023 год), научно-исследовательском семинаре кафедр дискретной математики и математической теории интеллектуальных систем механико-математического факультета и математической кибернетики факультета вычислительной математики и кибернетики МГУ имени М.В.Ломоносова (2023 год).

Достоверность и обоснованность результатов подтверждаются:

- четкостью формулировок утверждений и строгостью представленных доказательств;
- полнотой покрытия публикациями в рецензируемых журналах;
- апробацией на значительном числе семинаров и конференций.

Диссертация соответствует специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика (физико-математические науки): полученные результаты соотносятся с направлениями Теория алгебраических структур (полугрупп, групп, колец, полей, модулей и т.д.) и Теория дискретных функций и автоматов, теория управляемых систем. Изложенные результаты получены лично автором и являются новыми.

Считаю, что диссертация Кирилла Денисовича Царегородцева «Правильные семейства функций и порождаемые ими квазигруппы: комбинаторные и алгебраические свойства» удовлетворяет всем требованиям «Положения о присуждении ученых степеней в МГУ имени М.В.Ломоносова» и рекомендую ее к защите в диссертационном совете МГУ.011.4 на соискание ученой степени кандидата физико-математических наук по специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика.

Научный руководитель
кандидат физико-математических наук,
доцент кафедры математической теории
интеллектуальных систем
механико-математического факультета

МГУ имени М.В.Ломоносова

А.В. Галатенко

15.05.2025

Контактные данные. ФИО: Галатенко Алексей Владимирович.

Ученая степень: кандидат физико-математических наук.

Е-mail: agalat@msu.ru, тел.: 8 (495) 939-4637 (р.).

Специальность, по которой А.В. Галатенко была защищена кандидатская диссертация: 05.13.11 Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей (физико-математические науки).

Адрес места работы: 119991, ГСП-1, г. Москва, ул. Ленинские горы, д.1.

Должность: доцент кафедры математической теории интеллектуальных систем механико-математического факультета МГУ имени М.В.Ломоносова.

Подпись доцента кафедры Математической теории интеллектуальных систем механико-математического факультета МГУ им. М.В. Ломоносова удостоверяю.