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)

Квазигруппа является классическим объектом исследований в алгебре и комбинаторике. Это группоид с однозначным делением (как слева, так и справа). С комбинаторной точки зрения таблица умножения (конечной) квазигруппы представляет собой латинский квадрат — квадратную таблицу, каждая строка и каждый столбец которой содержат по одному экземпляру каждого элемента квазигруппы.

Применение латинских квадратов в шифровании (например, при табличном гаммировании) насчитывает многие сотни лет и обусловлено высокой стойкостью соответствующих шифров. К. Шеннон показал, что такие шифры обладают свойством совершенной секретности. С активным развитием криптографии в последней четверти XX века стали изучаться и другие возможности использования некоммутативных и неассоциативных алгебраических структур при синтезе криптопримитивов. Алгоритмы, основанные на квазигруппах, регулярно участвуют в конкурсах по выбору стандартов шифрования и хэширования. Также в последние годы стали появляться публикации с описаниями алгоритмов на основе n-квазигрупп, которые представляют собой обобщение квазигрупп на случай операции арности больше двух.

В отдельных примитивах используются квазигруппы порядка 2^{64} и выше. Табличное задание таких операций невозможно, здесь используется функциональный подход, при котором результат применения операции каждый раз вычисляется по значениям аргументов. Одним из способов реализации такого подхода является использование конструкции,

предложенной В.А. Носовым, и основанной на правильных семействах функций, то есть семействах n-арных булевых функций размера n, обладающих тем свойством, что для любой пары различных входных наборов найдется индекс i, такой что i-е компоненты этих наборов различны, но i-я функция семейства принимает на них одно и то же значение. Впоследствии этот подход был существенно обобщен, в том числе на случай логики произвольной значности.

Квазигруппы, построенные с помощью правильных семейств функций, можно отнести к так называемой многомерной криптографии, особый интерес к которой связан с тем, что алгоритмы шифрования с открытым ключом и электронной подписи, основанные на многомерных конструкциях, обладают высоким быстродействием, порождают подписи небольшой длины, а также способны противостоять квантовым атакам.

Предметом исследования К.Д. Царегородцева в представленной диссертационной работе являются свойства правильных семейств функций и их обобщений, а также криптографически значимые комбинаторно-алгебраические характеристики квазигрупп, порождаемых с помощью правильных семейств функций. Полученные автором результаты соответствуют мировому уровню исследований в данной области и отражают **актуальность и значимость работы.**

Общая характеристика работы. Представленная диссертационная работа состоит из введения, четырёх глав, заключения, списка литературы из 171 наименования, списка рисунков и списка таблиц. Общий объем работы составляет 143 страницы. **Введение** посвящено изложению целей и задач работы, обоснованию ее актуальности и практической значимости. Также во введении представлены основные результаты диссертации.

Первая глава называется «Основные определения и обозначения». После списка принятых обозначений приводятся определения алгебраических и комбинаторных объектов, изучаемых в работе (квазигруппы, d-квазигруппы, латинские квадраты) и связанных с ними

понятий, таких как изотопы, полные отображения и трансверсали. Также вводится терминология, связанная с действиями групп на множествах и с семействами дискретных функций и их преобразованиями. В разделе 1.3 вводится основной объект исследования — правильные семейства функций. Приводятся основные свойства правильных семейств функций, в частности, доказано обобщение критерия регулярности. Среди приводимых примеров следует отметить построенное автором правильное семейство квадратичных функций (правильность которого установлена в теореме 2, а строгий тип квадратичности в теореме 3). Далее рассматриваются критические важные для криптографических приложений характеристики квазигрупп: индекс ассоциативности, полиномиальная полнота, наличие (отсутствие) подквазигрупп. Доказан ряд утверждений о количестве ассоциативных троек, а также критерии того, что тройка элементов квазигруппы удовлетворяет тождеству ассоциативности.

Во **второй главе** правильные семейства функций сопоставляются с другими комбинаторными объектами, такими как одностоковые ориентации булевых кубов, и булевы сети с наследственно единственной неподвижной точкой. В терминах таких объектов сформулированы соответствующие условия, эквивалентные правильности семейства функций. Построенные автором естественные взаимно-однозначные соответствия между правильными семействами функций, одностоковыми ориентациями булевых кубов и булевыми сетями с наследственно единственной неподвижной точкой позволяют получить ряд результатов о порядке роста числа правильных семейств и доле булевых треугольных семейств от общего числа правильных семейств, а также построить новые примеры классов правильных семейств, названные автором рекурсивно-треугольными и локально-треугольными. Кроме того, вводится условие обобщенной правильности и показано, что оно эквивалентно отсутствию ортогональных аффинных подпространств специального вида (теорема 17).

В **Третьей главе** исследуются свойства правильных семейств. Описан стабилизатор множества правильных семейств относительно действий биекциями. Показано, что соответствующие биекции представляются в виде композиции перекодировок и перенумераций. Далее рассматривается характеристики преобразования булева куба, осуществляемого с помощью правильного семейства функций. Показано, что мощность полного прообраза элемента является четным числом. Найдены мощности образов отображений для двух специальных классов квадратичных правильных семейств. Следует отметить, что большая мощность образа исследуемого отображения является важным с точки зрения криптографических приложений свойством. Также в третьей главе рассматриваются свойства подстановок, порождаемых правильными семействами. Показано, что замыкание множества таких подстановок действует транзитивно на множестве Q^n, что также является важной криптографической характеристикой.

Четвертая глава посвящена алгоритмическим и вычислительным аспектам и содержит оригинальную схему шифрования, сохраняющего формат исходного сообщения, в основе которой лежат сдвиговые преобразования в квазигруппах, порожденных правильными семействами булевых функций. Здесь же приводится алгоритм распознавания правильности семейства булевых функций, основанный на проверке невыполнения свойства самодвойственности. В заключение главы представлен ряд результатов вычислительных экспериментов, касающихся правильных семейств (число булевых семейств различного вида, число классов эквивалентности) для небольших значений n, а также статистические данные об алгебраических свойствах (индекс ассоциативности, простота и аффинность) квазигрупп, построенных с помощью правильных семейств.

В **заключении** еще раз упоминаются задачи исследования и приводятся основные результаты работы:

1. установлено естественное соответствие между булевыми правильными семействами и одностоковыми ориентациями графов булевых кубов;

2. установлено естественное соответствие между булевыми правильными семействами 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 некоторых правильных семейств булевых функций получены точные значения мощности образа отображений, задаваемых этими правильными семействами;

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.

Также перечисляются возможные направления дальнейших исследований.

Представленные в работе результаты являются новыми и имеют важное значение для исследования свойств дискретных функций и неассоциативных алгебраических структур.

Возможность использования полученных результатов при разработке новых криптографических алгоритмов, а также при анализе стойкости существующих квазигрупповых систем защиты информации определяют их **практическую значимость**.

Диссертация носит теоретический характер, при этом полученные теоретические результаты гармонично дополнены экспериментальными данными. **Достоверность представленных в диссертации результатов** подтверждается строгостью математических доказательств, полнотой покрытия публикациями в рецензируемых математических журналах (9 статей, 8 из которых опубликованы в изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика) и апробацией на значительном числе научных семинаров и всероссийских и международных 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 А.Е. Панкратьев
16.05.2025

Контактные данные:
ФИО: Панкратьев Антон Евгеньевич.
Ученая степень: кандидат физико-математических наук.
E-mail: apankrat@intsys.msu.ru, тел. 8(495)939-4637 (р).
Специальность, по которой А.Е. Панкратьевым была защищена кандидатская диссертация: 01.01.06 Алгебра, логика и теория чисел (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