ОТЗЫВ официального оппонента
на диссертацию на соискание ученой степени
кандидата физико-математических наук
Царегородцева Кирилла Денисовича
на тему: «Правильные семейства функций и порождаемые ими квазигруппы: комбинаторные и алгебраические свойства»
по специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика

Актуальность темы диссертации. Квазигруппа представляет собой «группу без ассоциативности» и является классическим объектом исследований в алгебре и комбинаторике. Согласно формальному определению, квазигруппа — это группоид $(Q,*)$, такой что для любых элементов $a,\ b$ из множества Q уравнения $a*x=b$ и $y*a=b$ однозначно разрешимы. Таблица умножения (конечной) квазигруппы представляет собой латинский квадрат — комбинаторный объект, хорошо известный еще со времен Эйлера, поэтому термины «квазигруппа» и «латинский квадрат» часто используют в качестве синонимов.

Латинские квадраты широко используются в шифровании, их значение обусловлено доказанным Клодом Шенноном теоретическим свойством совершенной секретности шифра табличного гаммирования по латинскому квадрату. При этом для обеспечения необходимого уровня стойкости шифрсистем в криптографии часто бывают востребованы латинские квадраты больших размеров, которые невозможно задать табличным способом. В таких случаях можно использовать функциональный подход, при котором элемент латинского квадрата вычисляется как значение определенной функции от номера строки и номера столбца. Одна из таких конструкций была предложена В.А. Носовым. В ее основе лежит семейство n-арных булевых функций размера n, обладающее специальным свойством правильности (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.

При помощи правильных семейств функций можно строить, в частности, квадратичные квазигруппы, имеющие важные криптографические характеристики: при относительной простоте задания квазигрупповой операции задача выяснения разрешимости системы уравнений над квазигруппой, то есть, по существу, задача вскрытия соответствующего шифра, является вычислительно трудной.

Диссертационная работа К.Д. Царегородцева посвящена исследованию правильных семейств функций и свойств порождаемых ими квазигрупп. С учетом того, что в настоящее время квазигрупповая криптография является активно развивающимся направлением исследований, что подтверждается регулярным участием квазигрупповых систем в различных конкурсах криптографических стандартов, задачи, решенные в диссертационной работе К.Д. Царегородцева, являются **актуальными.**

Общая характеристика работы. Диссертационная работа включает введение, четыре главы, заключение, список литературы из 171 наименования, список рисунков и список таблиц. Общий объем работы составляет 142 страницы. Во **введении** изложены цели и задачи работы, обоснованы ее актуальность и практическая значимость, а также представлены основные результаты. В **первой главе,** которая называется «Основные определения и обозначения», приводятся используемые в работе обозначения из теории групп (квазигрупп) и теории дискретных функций (раздел 1.1). В разделе 1.2 введены понятия квазигруппы (d-квазигруппы) и семейства функций, рассмотрены преобразования таких семейств. Раздел 1.3 посвящен основному объекту исследования — правильным семействам функций. Приведены основные свойства и примеры правильных семейств функций, в том числе предложенная автором оригинальная конструкция, задающая параметрический класс квадратичных правильных семейств (Теорема 2). В разделе 1.4 указаны свойства квазигрупп, важные для криптографических

приложений: количество ассоциативных троек, полиномиальная полнота, наличие (отсутствие) подквазигрупп. В частности, представлен довольно полный обзор результатов по количеству ассоциативных троек.

Вторая глава называется «Эквивалентные условия правильности семейств» и посвящена различным способам характеризации правильных семейств функций в комбинаторно-геометрических терминах. К новым результатам относятся критерий правильности семейства булевых функций в терминах одностоковости ориентации соответствующего графа (Теорема 9), установление естественного взаимно-однозначного соответствия между правильными семействами булевых функций и булевыми сетями с наследственно единственной неподвижной точкой (теорема 12). В теореме 15 автор устанавливает характеризацию свойства правильности семейства функций k-значной логики в терминах клик обобщенных графов Келлера. Важной заслугой автора является установление естественных соответствий между правильными семействами функций и другими комбинаторными объектами, упомянутыми выше (булевы кубы с одностоковыми ориентациями, булевы сети с наследственно единственной неподвижной точкой), что позволяет переносить известные результаты с одних объектов на другие. Примерами результатов, полученных автором с помощью установления таких аналогий, являются оценки на количество правильных семейств, установление coNP-полноты задачи распознавания свойства правильности, а также эквивалентность правильности отсутствию самодвойственных подсемейств. В разделе 2.4 вводится условие обобщенной правильности, которое эквивалентно отсутствию ортогональных аффинных подпространств специального вида.

Третья глава содержит результаты о свойствах правильных семейств. В разделе 3.1 рассматриваются преобразования семейства функций при помощи двух биекций — «внутренней» и «внешней». Основным результатом является теорема 19, описывающая стабилизатор множества правильных семейств относительно данных преобразований. В разделе 3.2 показано, что

мощность полного прообраза элемента при отображении булева куба, реализуемом правильным семейством, является четным числом. Также найдены мощности образов отображений для двух классов квадратичных правильных семейств, одним из которых является представленная в главе 1 авторская конструкция (теорема 21), а другим — известная конструкция из циклически сдвинутых попарных произведений переменных (теорема 22). Следует отметить, что большая мощность образа правильного семейства свидетельствует о потенциальной широте класса порождаемых квазигрупп. Далее рассматриваются свойства подстановок, порождаемых правильными семействами, в частности, устанавливается криптографически важное свойство транзитивности соответствующего действия (теорема 25).

Четвертая глава — «Алгоритмические и вычислительные аспекты», посвящена практическим приложениям. В ней автор вводит оригинальную схему шифрования, сохраняющего формат исходного сообщения. Шифрование основано на сдвиговых преобразованиях в квазигруппах, порожденных правильными семействами булевых функций. Далее (раздел 4.2) приводится алгоритм проверки правильности семейства булевых функций, основанный на использовании характеризации правильности в терминах отсутствия самодвойственных подсемейств. Наконец, в разделе 4.3 приводятся результаты вычислительных экспериментов, включающих, в частности, таблицу мощностей множеств треугольных, рекурсивно треугольных, локально треугольных и правильных булевых семейств размеров до пяти включительно, количество классов эквивалентности правильных семейств малых размеров относительно множества преобразований, сохраняющих правильность, классификацию квазигрупп, порожденных с помощью правильных семейств, по значению индекса ассоциативности (мощности соответствующих классов). Кроме того, изучаются индексы ассоциативности квазигрупп, полученных из двух правильных семейств при помощи авторской конструкции (формула 4.2). Также приведены результаты экспериментального исследования свойств простоты и аффинности.

В **заключении** еще раз упоминаются задачи исследования, приводятся основные результаты работы и перечисляются следующие возможные направления дальнейших исследований:

1. Предложить способ построения широких классов правильных семейств с хорошими свойствами, в том числе и для логик значности $k>2$.

2. Предложить способ быстрого построения множества представителей всех правильных семейств размера $n+1$ с помощью представителей размера n и менее (с точностью до согласованных перенумераций и перекодировок).

3. Предложить альтернативные геометрические описания правильных семейств в k-значной логике, где $k>2$, которые были бы инвариантны относительно согласованных перенумераций и перекодировок.

4. Предложить полиномиальный алгоритм, принимающий на вход правильное семейство (в виде КНФ или полиномов Жегалкина) и параметрические подстановки и выдающий количество ассоциативных троек (или нижние и верхние границы), проверяющий полиномиальную полноту порождаемой квазигруппы, наличие или отсутствие подквазигрупп.

Степень обоснованности положений, выносимых на защиту, научных выводов и рекомендаций, сформулированных в диссертации, их достоверность и новизна: в главе 1 введено квадратичное правильное семейство, в главе 2 локально треугольные и рекурсивно треугольные семейства; получены новые критерии правильности семейств булевых функций и семейств функций логики произвольной значности, в том числе в терминах смежных областей исследований; получена характеризация преобразований, сохраняющих правильность (стабилизатор множества правильных семейств заданного размера); доказан ряд утверждений о мощности образа и прообраза при отображениях, определяемых правильными семействами. Также предложена новая схема шифрования и проведен ряд вычислительных экспериментов, важных для приложений.

Диссертация носит теоретический характер, при этом полученные теоретические результаты гармонично дополнены экспериментальными

данными. Следует отметить высокий уровень строгости рассуждений, четкость определений и формулировок утверждений. Доказательства корректные и в достаточной степени подробные. Тем самым, **выносимые на защиту положения являются обоснованными.**

Достоверность представленных в диссертации результатов обусловлена 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) и апробацией на значительном числе научных семинаров и всероссийских и международных конференций.

Замечания по диссертационной работе.

1. В первой главе следовало бы более четко отделить обзорную часть от собственных результатов диссертанта.
2. В работе используется термин лупа (в том числе упоминаются луповые кольца), при этом определения соответствующих алгебраических структур не приводятся.
3. К экспериментальным результатам работы было бы интересно добавить сравнение доли полиномиально полных квазигрупп, построенных с помощью конструкции автора, с долей полиномиально полных квазигрупп в классе всех квазигрупп заданного порядка.

Вместе с тем, указанные замечания не умаляют значимости диссертационного исследования. Диссертация отвечает требованиям, установленным Московским государственным университетом имени М.В.Ломоносова к работам подобного рода. Содержание диссертации соответствует специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика (по физико-математическим наукам), а также критериям, определенным пп. 2.1-2.5 Положения о присуждении ученых степеней в Московском государственном университете имени М.В.Ломоносова. Диссертационное исследование оформлено согласно

требованиям Положения о совете по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук Московского государственного университета имени М.В.Ломоносова.

Таким образом, соискатель Царегородцев Кирилл Денисович заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика.

Официальный оппонент:

Кандидат физико-математических наук,
ДОЦЕНТ кафедры теоретической кибернетики
Механико-математического факультета
ФГАОУ ВО «Новосибирский национальный
исследовательский государственный университет»

ТОКАРЕВА Наталья Николаевна Подпись:

Дата:

Контактные данные:

тел.: , e-mail:
Специальность, по которой официальным оппонентом
защищена диссертация:
01.01.09 — Дискретная математика и математическая кибернетика

Адрес места работы:

630090, Новосибирская область, г. Новосибирск, ул. Пирогова, д. 1