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 избранной темы. Конечные квазигруппы являются интересным с точки зрения криптографии объектом. К настоящему моменту предложено множество различных криптографических механизмов, в основе которых лежат квазигрупповые операции: начиная с работ Шеннона, который показал, что таблица умножения квазигруппы может использоваться для построения абсолютно стойкого шифра, и заканчивая современными работами, в которых рассматривается задача анализа и синтеза актуальных с практической точки зрения криптографических механизмов, таких как гомоморфное шифрование и постквантовые схемы подписи. При этом следует отметить, что для построения подобных механизмов требуются квазигруппы достаточно больших размеров. Задание квазигруппы с помощью таблицы в таком случае либо неэффективно, либо вообще не представляется возможным. Однако допустимо применить другие подходы, среди которых можно выделить функциональное задание квазигрупповой операции с помощью семейств дискретных функций, в частности, с помощью правильных семейств функций, которые были введены в работе В.А. Носова в 1998 г. и активно изучались В.А. Носовым и его учениками, А.Е. Панкратьевым и А.В. Галатенко. Правильные семейства являются основным объектом изучения в работе К.Д. Царегородцева.

Общая характеристика работы. Диссертация изложена на 142 страницах, состоит из введения, четырех глав, заключения, списка литературы из 171 источника, списка рисунков и списка таблиц.

Введение имеет стандартную структуру: в нем описываются основные цели и задачи работы, обосновывается актуальность и практическая значимость, приводятся основные результаты.

Первая глава посвящена введению основных определений и обозначений из теории квазигрупп и дискретных функций. В ней также содержится обзор основных результатов, касающихся правильных семейств функций, полученных В.А. Носовым, А.Е. Панкратьевым, А.В. Галатенко и другими соавторами. Помимо этого, доказываются и некоторые новые теоремы и утверждения, среди которых можно выделить новую конструкцию для порождения квазигрупповой операции (теорема 1, замечание 11) и пример нового класса квадратичных правильных семейств (теорема 2, теорема 3).

Во второй главе изучаются различные эквивалентные определения правильности семейства, часть из которых работает только в булевом случае, а другие — и в более общем случае k-значной логики. В первой группе утверждений можно выделить эквивалентность между правильными булевыми семействами и т.н. «одностоковыми ориентациями булевых кубов» (теорема 9), а также между упомянутыми семействами и булевыми сетями с наследственно единственной неподвижной точкой (теорема 12). Используя полученные естественные биективные соответствия, автору удается перенести часть результатов из развитой теории одностоковых ориентаций и булевых сетей на «язык» правильных семейств функций. В частности, удается построить новые классы семейств (рекурсивно треугольные (раздел 2.1.4), локально треугольные (раздел 2.2.1)), доказать оценки на мощности некоторых классов правильных семейств. В заключении главы приводится альтернативная характеризация правильных семейств в k-значном случае: показывается взаимно-однозначное соответствие между правильными семействами в k-значной логике и кликами определенного размера в специально построенном графе. Также вводится понятие обобщенно правильного семейства и доказывается его связь со свойствами

ортогональности аффинных подпространств (в случае $k = 2$ полученное описание является критерием правильности).

Третья глава посвящена доказательству различных свойств правильных семейств. Получено полное описание стабилизатора множества правильных семейств относительно действий пар биекций (раздел 3.1), изучены характеристики различных отображений, задаваемых правильными семействами функций, такие как мощность образов: показано, что мощность образа отображения, заданного правильным булевым семейством, всегда четна (теорема 20); вычислены мощности образов некоторых конкретных квадратичных семейств (теоремы 21, 22). В конце главы (раздел 3.3) рассмотрены некоторые алгебраические свойства подстановок, задаваемых правильными семействами: показана замкнутость множества «правильных подстановок» относительно операции обращения, четность мощности множества неподвижных точек, а также транзитивность действия таких подстановок на множестве двоичных векторов длины n.

Четвертая глава является наиболее «практико-ориентированной». В рассматриваются различные алгоритмические аспекты, в частности предлагается алгоритм шифрования, сохраняющего формат сообщений (т.н. FPE-шифры) на основе квазигрупповой операции; описывается упрощенный с точки зрения сложности вычислений по сравнению с «наивным» алгоритм распознавания правильности семейства булевых функций, который существенным образом опирается на одно из эквивалентных описаний правильных булевых семейств. Раздел 4.3 посвящен изложению результатов вычислительных и статистических экспериментов: приведено точное число правильных семейств булевых функций в общем случае для $n = 2,3,4,5$ и точное число для подклассов (треугольные, локально треугольные, рекурсивно треугольные семейства); изучены показатели неассоциативности квазигрупп, порожденных с помощью конструкции, предложенной автором в первой главе диссертации, а также свойства аффинности и простоты полученных квазигрупп.

В **заключении** напоминаются основные результаты диссертации, а также приводится рад направлений дальнейших исследований.

Степень обоснованности положений, выносимых на защиту, научных выводов и рекомендаций, сформулированных в диссертации, их достоверность и новизна: диссертация носит преимущественно теоретический характер. Определения введены строго, формулировки утверждений и теорем корректны, доказательства верны и достаточно подробны, что свидетельствует о высокой степени обоснованности положений, выносимых на защиту. 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 ряде научных семинаров и всероссийских и международных конференций. Все результаты являются новыми.

Результаты других авторов, упомянутые в тексте диссертации, отмечены ссылками на соответствующие публикации.

Замечания по диссертационной работе.

1.

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:

Доктор физико-математических наук, доцент,
ПРОФЕССОР кафедры 252
Института искусственного интеллекта
ФГБОУ ВО «МИРЭА - Российский технологический университет»

КАМЛОВСКИЙ Олег Витальевич Подпись:

Дата:

Контактные данные:

тел.: , e-mail:
Специальность, по которой официальным оппонентом
защищена диссертация: 6.4.4. Теоретическая криптография
Адрес места работы:

119454, г. Москва, проспект Вернадского, д. 78