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. Квазигруппой называется группоид $(Q,*)$, такой что для любых элементов a, b из множества Q уравнения $a*x=b$ и $y*a=b$ однозначно разрешимы. Содержательно это означает, что при произвольной фиксации произвольного аргумента операции * получающаяся одноместная функция является биекцией. Если множество Q конечно, таблица Кэли операции * представляет собой латинский квадрат, то есть в каждой линии (строке или столбце) элементы попарно различны, и наоборот, произвольный латинский квадрат является таблицей Кэли операции, задающей конечную квазигруппу.

Свойство обратимости операции * по каждой переменной востребовано в криптографических приложениях. К. Шеннон доказал, что табличное гаммирование по латинскому квадрату обладает свойством совершенной секретности, то есть знание шифр-текста не дает злоумышленнику никакой информации об открытом тексте. При этом длина ключа должна быть не меньше длины открытого текста. Известны и более практичные криптосистемы, длина ключа в которых является константой. Квазигрупповая криптография активно изучается в России (отметим результаты В.А. Артамонова, В.Т. Маркова, А.В. Черемушкина, В.А. Носова) и за рубежом, в Македонии (группа С. Марковского), Норвегии (Д. Глигороски с коллегами), в Индии.

В ряде случаев, например, при построении криптографических хеш-функций, шифров с открытым ключом или систем электронной подписи, возникает необходимость использования квазигрупп большого порядка. На

практике это означает невозможность табличного задания операции *. В.А. Носов предложил задавать квазигруппы с помощью так называемых правильных семейств функций. Такой способ позволяет добиться значительной экономии памяти (особенно в случае функций с низкой формульной сложностью) при несущественном росте времени вычисления; кроме того, за счет вариации внутренних параметров одно правильное семейство порождает экспоненциальное от размера число квазигрупп.

Понятие правильного семейства является ключевым для диссертации, поэтому кажется необходимым привести определение. Пусть k, n — натуральные числа, f_1, …, f_n — функции k-значной логики от n переменных. Семейство (f_1, …, f_n) называется правильным, если для любой пары различных входных наборов s, t найдется индекс i, такой что s_i не равно t_i, но $f_i(s)=f_i(t)$. Очевидным примером является семейство, состоящее из констант, значительное число более содержательных примеров приведено в диссертации.

В работе К.Д. Царегородцева получены интересные продвижения в области изучения правильных семейств функций: установлены новые свойства таких семейств, обнаружены и изучены новые классы примеров правильных семейств, введена новая конструкция для задания квазигрупп, отличная от конструкции В.А. Носова, и на основе этой конструкции предложен новый класс шифров, сохраняющих формат. Задачи, решенные в диссертации, являются **актуальными**, а полученные результаты — **значимыми**.

Общая характеристика работы. Объем диссертации К.Д. Царегородцева составляет 142 страницы. Работа состоит из введения, четырех глав, заключения, списка литературы из 171 источника, списка рисунков и списка таблиц. Во **введении** описываются цели работы, обосновывается актуальность и практическая значимость, приводятся основные результаты. **Первая глава** называется «Основные определения и обозначения». Помимо определений и обозначений из области квазигрупп и

правильных семейств функций в ней приведены достаточно полные и подробные обзоры результатов по правильным семействам функций (раздел 1.3) и требованиям к квазигруппам в криптографии (раздел 1.4). Кроме того, приведены и оригинальные результаты, полученные автором, ключевыми из которых являются новая конструкция для порождения квазигрупп с помощью правильных семейств функций (замечание 11) и новое квадратичное правильное семейство (теорема 2).

Вторая глава называется «Эквивалентные условия правильности семейств». В ней автор приводит ряд содержательных новых критериев правильности. Часть из них работает в только в случае семейств булевых функций (эквивалентность правильности и одностоковости некоторой ориентации булева куба, теорема 9; эквивалентность правильности и существованию наследственно единственной неподвижной точки некоторой булевой сети, теорема 12), часть является универсальной (кликовое представление, теорема 15). Ценность критериев, в частности, определяется возможностью перевода известных результатов об одностоковых ориентациях и булевых сетях с наследственно единственными неподвижными точками на язык правильных семейств булевых функций. Таким образом получаются оценки на мощность множества правильных семейств, утверждения о coNP-полноте задачи проверки правильности, классы локально треугольных и рекурсивно треугольных правильных семейств, характеризация правильности в терминах отсутствия самодвойственных подсемейств. Завершает главу раздел про обобщение свойства правильности в терминах неортогональности аффинных подпространств. Этот раздел ярко иллюстрирует различие булева случая и случая k-значной логики при $k>2$.

Третья глава называется «Свойства правильных семейств». В этой главе сперва описывается стабилизатор множества правильных семейств относительно некоторого естественного класса преобразований (теорема 19; это одно из наиболее технически сложных утверждений работы, ярко демонстрирующее широту технического арсенала автора), затем изучаются

характеристики отображений, реализуемых правильными семействами: утверждение о четности мощности полного прообраза любого элемента (теорема 20), а также утверждения о мощности образа двух важных классов отображений — квадратичного семейства, введенного в первой главе (теорема 21; здесь доказано, что мощность максимально возможная) и известного квадратичного семейства, каждая функция в котором задается формулой сложности 3 (теорема 22). Мощность образа семейства является важной характеристикой, в значительной степени определяющей богатство класса порождаемых квазигрупп. Завершает главу раздел про перестановки, порождаемые правильными семействами. Здесь хочется выделить теорему 25, утверждающую, что группа перестановок, порождаемых правильными семействами, действует транзитивно на соответствующем множестве. Транзитивность действия является слабой аппроксимацией свойства совершенной секретности.

Четвертая глава называется «Алгоритмические и вычислительные аспекты». В ней сперва вводится класс симметричных шифров, сохраняющих формат исходного сообщения (FPE-шифров), основанных на правильных семействах функций. Затем описывается алгоритм проверки правильности семейства булевых функций, оптимизированных по сравнению с проверкой по определению (и существенно использующий критерий правильности в терминах отсутствия самодвойственных подсемейств из второй главы). Такой алгоритм может быть использован для подбора параметров алгоритма шифрования. В третьем разделе приводятся результаты вычислительных экспериментов, существенных с точки зрения безопасности шифра: число правильных семейств булевых функций в общем случае и для некоторых подклассов (характеристика, определяющая мощность множества ключей), показатели неассоциативности порожденных квазигрупп (чем выше неассоциативность, тем лучше; к сожалению, полученные в эксперименте значения далеки от рекордных), распределение порождаемых квазигрупп по классам в зависимости от простоты/непростоты и аффинности/неаффинности

(желаемыми свойствами являются простота и неаффинность; оказывается, уже при размере семейства 3 порождается значительное число простых неаффинных квазигрупп).

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

Диссертация носит преимущественно теоретический характер. Определения введены четко и строго, формулировки утверждений корректные, доказательства верные, строгие и достаточно подробные и понятные, что свидетельствует о **высокой степени обоснованности положений, выносимых на защиту, научных выводов и рекомендаций, представленных в диссертации**.

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.

Научная новизна. Все результаты являются новыми. К.Д. Царегородцевым введены новые классы правильных семейств: квадратичное семейство из главы 1 и локально треугольные и рекурсивно треугольные семейства из главы 2; получены новые содержательные критерии правильности семейств булевых функций и семейств функций логики произвольной значности; описан стабилизатор множества правильных семейств заданного размера; изучены характеристики образа и прообраза под действием правильных семейств; предложена новая схема шифрования, сохраняющего формат.

Замечания по диссертационной работе.

1. Название первой главы кажется не совсем удачным и не в полной мере отражающим реальное содержание.
2. Во второй главе хотелось бы более подробно обсудить вопрос переноса результатов, появляющихся в булевом случае благодаря полученным критериям, на случай логики произвольной значности. В частности, было бы интересно собрать известные критерии правильности семейств булевых функций, одностоковости ориентаций и существования наследственно единственной неподвижной точки в булевом случае и проверить, какие из критериев можно естественным образом перенести на логику большей значности.
3. В продолжение прошлого замечания кажется немного странным, что автор не упомянул обобщение нижней оценки мощности множества правильных семейств на k-значный случай, опубликованную одним из научных руководителей.
4. В четвертой главе хотелось бы увидеть чуть больше экспериментальных данных. В частности, было бы интересно узнать, правильность семейств какого размера может быть установлена с помощью предложенного автором алгоритмом «за разумное время», а также изучить характеристики квазигрупп, сгенерированных с помощью случайных правильных семейств более высокого порядка.

Вместе с тем, указанные замечания в значительной степени являются пожеланием к направлению дальнейших исследований, не носят существенный характер и не снижают положительного впечатления от диссертации. 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 высшей математики и физики
Институт математики, информатики и физики
ФГБОУ ВО «Волгоградский государственный
социально-педагогический университет»»

ЩУЧКИН Николай Алексеевич Подпись:

Дата:

Контактные данные:

тел.: 7(8442)945533, e-mail:
Специальность, по которой официальным оппонентом
защищена диссертация:
01.01.06 — Математическая логика, алгебра и теория чисел

Адрес места работы:

400001, Волгоградская область, г. Волгоград, ул. Академическая, д. 12