

## ОТЗЫВ

на автореферат диссертации Царегородцева Кирилла Денисовича на тему  
«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

Конечные квазигруппы представляют интерес для криптографии, так как с их использованием можно строить различные криптографические примитивы, например, блочные и поточные шифры, функции хэширования, схемы распределения ключей, схемы электронной подписи. При этом важно уметь относительно компактно и эффективно задавать квазигруппы больших размеров (порядка  $2^{64} \times 2^{64}$  и больше). Табличное задание квазигруппы в таком случае не представляется возможным, но допустимы другие подходы, такие как изотопии групп, «сборка» большой квазигруппы из малых с помощью конструкций произведений, а также, функциональное задание квазигрупповой операции 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. Последний подход является основной темой исследований диссертации К.Д. Царегородцева.

**В первой главе** вводятся основные используемые понятия, освещаются известные результаты, касающиеся правильных семейств. Также вводится новый способ порождения квазигрупп с помощью правильных семейств и изучаются некоторые характеристики получаемых квазигрупп. Приводится новое семейство, состоящее из квадратичных булевых функций, доказываются его правильность и изучается его степень квадратичности. Подобные семейства важны для приложений, поскольку задаются относительно компактными формулами.

**Вторая глава** посвящена доказательствам эквивалентности свойства правильности и иных интересных свойств, изучаемых в других разделах математики. Рассмотрены одностокковые ориентации булева куба, булевы сети с наследственно единственными неподвижными точками, клики заданного размера в графах особого вида (обобщенные графы Келлера). Для каждого класса объектов получено биективное соответствие между объектами класса и правильными семействами. Полученные соответствия позволили автору «перевести» известные утверждения на язык правильных семейств и получить их обобщения (например, правильность рекурсивно треугольных и локально треугольных семейств).

**В третьей главе** изучаются свойства правильных семейств. Отдельно можно выделить результат о стабилизаторе правильных семейств в классе биективных преобразований и вычисление мощности образа двух квадратичных булевых правильных семейств, что, в свою очередь, позволяет оценить снизу число различных квазигрупп, порождаемых семейством с помощью одной из конструкций.

**В четвертой главе** изложены практические результаты. Предложен новый квазигрупповой алгоритм шифрования с сохранением формата сообщений (FPE-шифра), основанный на конструкции из первой главы. Приведены результаты статистических экспериментов для различных характеристик квазигрупп, порожденных правильными

семействами, такие как индекс ассоциативности, простота, неаффинность, полиномиальная полнота. Экспериментально найдены мощности множеств некоторых классов булевых правильных семейств небольшого размера.

Считаю, что автору диссертации удалось получить интересные и содержательные результаты, имеющие теоретическую значимость и практическую ценность.

Автореферат диссертации достаточно полно отражает результаты работы, которые представлялись на 10 конференциях и 6 научных семинарах. По теме диссертации опубликовано 9 статей в рецензируемых журналах, включая 6 статей в изданиях, входящих в ядро РИНЦ, и 2 статьи в изданиях из дополнительного списка Московского государственного университета имени М.В. Ломоносова.

**В качестве замечаний к автореферату можно отметить следующие.**

1. Не все используемые понятия являются общеизвестными. В частности, стоило бы более подробно изложить ключевые для второй главы понятия одностокковой ориентации булева куба и булевой сети с наследственно неподвижной общей точкой.

2. К изложению ключевых результатов было бы целесообразно добавить содержательные комментарии, поясняющие значимость того или иного результата.

Отмеченные замечания не являются существенными и не снижают общую положительную оценку работы.

Судя по автореферату, диссертация К.Д. Царегородцева является завершенной научно-квалификационной работой и соответствует требованиям, предъявляемым к диссертациям на соискание учёной степени кандидата физико-математических наук по специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика. Считаю, что К.Д. Царегородцев заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика.

Рецензент:

Кандидат физико-математических наук,  
заместитель руководителя службы сертификации  
по научно-техническому сотрудничеству,  
ООО «Код Безопасности»  
КОРЕНЕВА Алиса Михайловна

Адрес места работы:

115230, Россия, Москва, 1-й Нагатинский проезд, д. 10, стр. 1  
ООО «Код Безопасности», Служба по сертификации, ИБ и криптографии  
Тел.: 7(495)9823020; e-mail: info@securitycode.ru

Подпись сотрудника А.М. Кореновой удостоверяю: