О Т З Ы В

официального оппонента о диссертационной работе

Тумайкина Ильи Николаевича

«Коды Рида – Маллера как групповые коды»,

представленной на соискание ученой степени

кандидата физико-математических наук

Теория кодирования, как одна из наиболее математизированных прикладных областей науки с самого ее зарождения очень тесно связана с алгеброй, в частности, с теориями конечных полей, конечных колец и алгебр. Поэтому теоретические исследования в этих разделах алгебры были и остаются важными и актуальными направлениями развития как для самой алгебры, так и для применения их результатов для дальнейшего развития теории кодирования.

В частности, даже такой важный и часто используемый в приложениях класс кодов как линейные коды Рида – Маллера и их обобщения продолжает служить источником весьма актуальных алгебраических задач.

Именно исследованию алгебраической структуры обобщенных кодов этого класса и посвящена диссертация Тумайкина И. Н., а именно, изучению строения так называемых «базисных кодов Рида – Маллера», рассматриваемых как идеалы групповой алгебры конечной примарной p-группы над произвольным конечным полем характеристики p. Конкретно, исследуется последовательность степеней фундаментального идеала этой групповой алгебры (который в данном случае совпадает с радикалом Джекобсона).

Диссертация состоит из введения, шести разделов основного текста, заключения, списка цитируемой литературы и приложения.

Во введении кратко излагаются основные понятия исследуемой области, постановки задач и основные результаты диссертации. Изложение четкое и понятное, дает верное представление о сути рассматриваемых задач и полученных автором результатов.

Первый раздел основного текста носит вводный характер. Он содержит основные обозначения и определения, используемые далее в тексте диссертации, а также некоторые базовые результаты, предваряющие следующие разделы.

Коды Рида – Маллера, а также обобщающие их базисные коды Рида – Маллера определяются как некоторые идеалы специального вида групповой алгебры QH, где Q – конечное поле характеристики p порядка p^l, H – элементарная p – группа, изоморфная аддитивной группе поля Q и задано подполе P поля Q, состоящее из p^λ.

Ранее другими авторами было доказано, что при $\lambda=1$ коды Рида – Маллера совпадают со степенями радикала групповой алгебры PH, а базисные коды Рида – Маллера совпадают со степенями радикала групповой алгебры QH.

В разделах 2 – 6 диссертации излагаются результаты автора, доказывающие, что при $\lambda > 1$ совпадение этих кодов со степенями соответствующих радикалов имеет место только в тривиальных случаях, а также устанавливающие связи (описываются включения множеств) этих кодов и степеней соответствующих радикалов групповых алгебр.

В разделе 2 устанавливается отличие степеней радикала от базисных кодов Рида – Маллера, а в разделе 6 аналогичные факты устанавливаются для обычных кодов Рида – Маллера. В промежуточных между этими разделами текста разделах от третьего до пятого излагаются результаты автора, описывающие какие степени радикала содержатся в коде, а также какие степени радикала содержат соответствующий код. В этих разделах диссертации излагаются также все результаты вспомогательного характера, необходимые для доказательства основных утверждений автора. В частности, построены базисы кодов Рида – Маллера, отличные от стандартно используемых, но более удобные для изучения исследуемых алгебраических вопросов о структуре этих кодов.

На основании доказанных автором утверждений о взаимных включениях кодов Рида – Маллера (обычных и базисных) и степеней радикала соответствующей групповой алгебры строится граф включений этих множеств. В качестве наглядной иллюстрации этих результатов автор приводит в приложении фрагмент такого графа, полученный с помощью компьютерной программы, для случая $p = 2, l = 9, \lambda= 3$, а также полностью граф для случаев $p = 2, l = \lambda = 4$ и $p = \lambda = 2$.

Автореферат диссертации правильно и достаточно полно отражает ее содержание.

К недостаткам работы следует отнести следующие мелкие погрешности текста: на стр. 11 в 5-й строек сверху дважды написано $t\in\mathbb{Z}$, хотя должно быть $t\in N$; на стр. 18 в 15-й строке сверху автор пишет «Как показано далее», а следовало бы указать точнее – например, «Как будет показано далее в теореме 3.3»; вводимое на стр. 8 обозначение $\pi=p\hat{}\lambda$ вначале несколько смущает читателя поскольку широко принятое в математике обозначение символом π уникального трансцендентного числа здесь обозначает натуральную степень любого простого числа p, натуральный показатель которой часто также использует греческую букву λ; в определении 2.3 на стр. 11 говорится об упорядочении «на множестве π-координат», хотя по смыслу дела это соответствует упорядочению «на множестве m-координат», как это и используется далее по тексту.

Кроме того, список литературы ограничен всего 13-ю работами, три из которых принадлежат автору. Для более точного представления о других исследованиях в данной области, а также для более точного отражения ширины и глубины знаний автора в данной области следовало бы привести больше работ в списке литературы, а также шире отразить знания автора в данной области в основном тексте диссертации или во введении.

Указанные недостатки не изменяют общего положительного впечатления от данной работы. Результаты диссертации являются новыми, получены автором самостоятельно и представляют несомненный научный интерес. Все утверждения автора снабжены корректными логическими доказательствами. Тем самым, в диссертации Тумайкина И.Н. получен исчерпывающий ответ на вопрос о соотношениях включения между основными и

базисными кодами Рида – Маллера и степенями радикала соответствующей групповой алгебры.

Текст диссертации показывает, что автор хорошо владеет методами алгебры, комбинаторики и теории чисел. Результаты диссертации могут быть использованы в спецкурсах по общей алгебре и ее приложениям, читаемых в МГУ, а также в курсах алгебраической теории кодирования, читаемых на кафедре ИУ8 МГТУ им. Н.Э. Баумана.

Они могут быть полезны также при изучении алгебраических свойств криптографических преобразований отечественных стандартов шифрования «Кузнечик» (ГОСТ Р 34.12-2015) и хэширования «Стрибог» (ГОСТ Р 34.11-2012), а также для построения алгебраических методов криптоанализа данных алгоритмов и аналогичных международных криптографических стандартов (AES, SHA-1, SHA-256, PRESENT, SPECK, SIMON и др.).

Считаю, что диссертационная работа «Коды Рида – Маллера как групповые коды» удовлетворяет всем требованиям «Положения о порядке присуждения ученых степеней» ВАК, а ее автор Тумайкин И.Н. заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 01.01.06 – математическая логика, алгебра и теория чисел.

Автор отзыва – Лебедев Анатолий Николаевич, кандидат физико-математических наук, старший научный сотрудник.

Место работы, должность: Национальный исследовательский университет «МГТУ им. Н.Э. Баумана», доцент кафедры Информационной безопасности (ИУ8)

Домашний адрес и телефон: 107140, Москва, ул. Краснопрудная, д. 26, кв. 56, тел. 985.766.80.26

Электронная почта: lan@lancrypto.com

Кандидат физико-математических наук,
старший научный сотрудник,
доцент кафедры ИУ8 МГТУ им. Н.Э. Баумана А. Н. Лебедев

Подпись Лебедева А.Н. удостоверяю
Руководитель НУК ИУ МГТУ им. Н.Э. Баумана В. А. Матвеев

«01» июня 2017г.