УТВЕРЖДАЮ
Первый проректор федерального
государственного автономного
образовательного учреждения высшего
образования «Национальный
исследовательский университет
«Высшая школа экономики»
д.э.н., профессор Вадим Валерьевич Радаев

«11» октября 2021 г.

ОТЗЫВ

ведущей организации на диссертацию **Лебедева Владимира Сергеевича** «Коды для каналов множественного доступа и задачи комбинаторного поиска», представленную на соискание учёной степени доктора физико-математических наук по специальности 05.13.17 – теоретические основы информатики

Актуальность темы диссертации

Диссертация посвящена разработке новых методов и алгоритмов кодирования информации в каналах множественного доступа, позволяющих на основании комбинаторного подхода получать более точные оценки характеристик кодов, используемых для передачи и защиты информации в таких каналах. Также в диссертации рассматриваются обобщения хорошо известных и ключевых задач как для теории передачи по каналам множественного доступа, так и комбинаторного (группового) поиска. Так, классическая задача поиска одного дефектного элемента с безошибочной обратной связью, которая называется задачей Улама или задачей Реньи-Улама, в диссертации обобщается на q-ичный случай. Другим примером является задача

построения кодов для дизъюнктивного канала множественного доступа. В диссертации изучаются коды, свободные от перекрытий, которые являются естественным обобщением дизъюнктивных кодов. Получением верхних границ (или границ несуществования) для скорости таких кодов занимались многие исследователи, однако в диссертации большинство известных результатов было существенно улучшено.

Третьей известной задачей как для каналов множественного доступа, так и для комбинаторного поиска является задача построения сигнатурных кодов для суммирующего канала множественного доступа, или, что тоже самое, построение алгоритмов поиска фальшивых монет на точных весах. Эта задача изучалась сначала в комбинаторной теории поиска, ею занимались такие известные математики как Эрдеш и Реньи, а затем она была переоткрыта в теории кодов для каналов множественного доступа. Таким образом, в диссертации исследуется много нерешенных задач теории передачи информации по каналам множественного доступа, что делает тему диссертации несомненно актуальной.

Новизна полученных результатов и выводов

Научная новизна работы состоит в том, что в ней впервые комбинаторный подход к задачам поиска переосмыслен с точки зрения методов теории кодирования, что позволило получить важные научные результаты как для теории комбинаторного поиска, так и для теории передачи информации по каналам множественного доступа. В частности, предложен новый метод исправления ошибок для q-ичного канала с безошибочной обратной связью. Предложенный алгоритм является оптимальным для доли ошибок в канале, большей 1/q. Впервые введено понятие композиционного расстояния и получена граница на скорость кодов с таким композиционным расстоянием, что позволило получить новые границы для скорости кодов без перекрытий, являющихся обобщением кодов для дизъюнктивных каналов множественного доступа. Отметим, что эти коды возникли в криптографии

как задача о минимизации числа секретных ключей при фиксированном числе пользователей.

Также предложен новый алгоритм поиска для канала множественного доступа с двумя входами, позволяющий получить оптимальную константу при главном члене для общего числа пользователей. Успех в разработке такого алгоритма позволяет рассчитывать на дальнейшее продвижение в этом направлении и разработку алгоритмов для поиска большего числа дефектных элементов.

Апробация работы и публикации

Положения и выводы, сформулированные в диссертации, получили квалифицированную апробацию на международных и российских научных конференциях и семинарах. Они опубликованы в изданиях, большинство из которых индексируется системами Web of Science и Scopus. Основные результаты опубликованы в 31 печатной работе, из которых 21 в работах, индексируемых базами данных WoS/Scopus, из них 16 статей в рецензируемых журналах и 5 статей в сборниках трудов конференций. Таким образом, результаты диссертации своевременно и достаточно полно опубликованы.

Обоснованность научных положений и выводов, сформулированных в диссертации

Все научные положения и выводы диссертации обоснованы строгими математическими доказательствами. Их достоверность также подтверждается публикациями результатов исследования в рецензируемых научных изданиях, в том числе, рекомендованных ВАК, и презентацией результатов на различных международных и российских научных конференциях.

Соответствие содержания диссертации автореферату и указанной специальности

Автореферат диссертации правильно и достаточно полно отражает ее содержание. Соответствие выбранной специальности подтверждается тем, что тема диссертации - исследования свойств кодов, используемых для передачи информации по каналам множественного доступа, традиционно является одной из ключевых тем в теоретических основах информатики (специальность 05.13.17 – теоретические основы информатики).

Значимость результатов для науки и производства

Диссертационная работа вносит крупный вклад в решение описанных выше задач, поскольку в ней впервые предложен комбинаторный подход рассмотрения этих задач с точки зрения методов теории кодирования, позволивший получить важные научные результаты. Данная работа является теоретической. Тем не менее, выводы и подходы диссертации могут быть полезны для различного рода приложений. Практическая ценность полученных результатов определяется тем, что они могут применяться в дальнейших исследованиях в области теории кодирования, криптографии и комбинаторного поиска.

Замечания по диссертационной работе

Имеется несколько замечаний к диссертационной работе.

1) Одним из предметов исследований третьей главы являются коды, свободные от перекрытий. Автор вводит понятие композиционного расстояния, которое правильно называть не расстоянием, а весом или нормой, так как это одноместная, а не двухместная функция.

2) Там же, в третье главе, получена рекуррентная верхняя граница для скорости кодов, свободных от перекрытий, теорема 8. К сожалению, автор не исследовал детально, что даст эта рекуррента в наиболее простом, как нам

кажется, случае w=r, когда представляется возможным осуществить рекуррентный спуск без особо громоздких вычислений.

Отмеченные недостатки не умаляют общего положительного впечатления от диссертационной работы.

Вывод

Диссертационная работа Лебедева Владимира Сергеевича «Коды для каналов множественного доступа и задачи комбинаторного поиска» является законченной научно-квалификационной работой на актуальную тему, в которой на основании выполненных диссертантом исследований разработаны теоретические положения, совокупность которых можно квалифицировать как научное достижение в области теоретических основ информатики. Она соответствует п.11 специальности 05.13.17 – теоретические основы информатики и удовлетворяет требованиям пунктов 9-10 Положения о присуждении ученых степеней, утвержденного постановлением Правительства РФ от 24 сентября 2013 года № 842. Ее автор В.С. Лебедев несомненно заслуживает присуждения ему ученой степени доктора физико-математических наук по указанной специальности.

Отзыв подготовлен доктором технических наук, профессором Московского института электроники и математики им.А.Н.Тихонова федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет «Высшая школа экономики» Нефедовым Сергеем Игоревичем.

Отзыв рассмотрен и одобрен на заседании НТС Московского института электроники и математики им. А.Н.Тихонова федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет «Высшая школа экономики», протокол № 1 от «25» сентября 2021 года.

Сведения о ведущей организации: Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Высшая школа экономики» (НИУ ВШЭ)

Адрес: 101000 г. Москва, ул. Мясницкая, 20.
Тел.: (495) 771-32-32
Электронная почта: hse@hse.ru
Сайт: http://www.hse.ru

Заместитель директора
МИЭМ НИУ ВШЭ
к.т.н., доцент Аксенов Сергей Алексеевич

Профессор
МИЭМ НИУ ВШЭ
д.т.н., профессор Нефедов Сергей Игоревич

Подпись заверяю
ПО ДОВЕРЕННОСТИ ПО КАДРОВОМУ ДЕЛОПРОИЗВОДСТВУ
И КАДРОВОМУ АДМИНИСТРИРОВАНИЮ
ПЕРСОНАЛА
Стоянова Т. И.