**ОТЗЫВ**

официального оппонента о диссертации В. С. Лебедева «Коды для каналов множественного доступа и задачи комбинаторного поиска», представленной на соискание учёной степени доктора физико-математических наук по специальности 05.13.17 – теоретические основы информатики

Тема диссертации является актуальной, поскольку связана с разработкой новых методов и алгоритмов кодирования информации в канале множественного доступа (КМД), позволяющих на основании комбинаторного подхода получать более точные оценки характеристик некоторых кодов, используемых для передачи и защиты информации. Свойства КМД активно изучаются на протяжении многих десятилетий. Так, к примеру, активно исследуется проблема обеспечения помехоустойчивости информационных коммуникаций для целей передачи информации. Данную задачу с безошибочной обратной связью называют задачей Улама, или задачей Реньи-Улама, и она имеет много важных приложений. Другой пример дает задача построения кодов для дизъюнктивного КМД. Получением верхних и нижних границ для скорости таких кодов занимались многие исследователи, однако такие точные как в диссертации результаты не были получены. Также очень популярна задача для суммирующего КМД. Вместе с тем, имеется и много нерешенных задач, актуальных для теории информации, которые описываются в терминах КМД и являются предметом рассмотрения настоящей диссертации.

Целью диссертационной работы является разработка подходов и методов исследования свойств кодов, используемых для передачи и защиты информации, в том числе обслуживающих некоторые каналы множественного доступа.

В первой главе рассматривается задача передачи информации по q-ичному каналу с
безошибочной обратной связью. Описан алгоритм r удаления. Доказано, что алгоритм 1 удаления является оптимальным для доли ошибок в канале, большей 1/q. Данный алгоритм позволил перенести результаты Берлекампа с двоичного на q-ичный случай. Оценивается число q-ичных последовательностей, содержащих подблок 00 ровно r раз. Предложенный метод оценки дает

возможность исследовать число последовательностей с другими ограничениями. В конце первой главы описан обобщенный алгоритм 1 удаления. Доказано, что обобщенный алгоритм 1 удаления позволяет передавать больше сообщений, чем алгоритм 1 удаления на некотором интервале значений доли ошибок. Приведены численные результаты, показывающие, что на этом интервале обобщенный алгоритм очень близок к оптимальному для больших значений q. Во второй главе строится алгоритм поиска двух дефектных элементов, позволяющий получить формулу для общего числа элементов, среди которых можно найти два дефектных. Из данной формулы вытекает, что константа при главном члене асимптотики для общего числа элементов является оптимальной. Все алгоритмы, предложенные ранее, давали константу меньше единицы. Кроме того, решается задача поиска одного из нескольких дефектов для разных случаев модели тестирования. Подобная постановка задачи мне кажется весьма интересной. В третьей главе изучаются коды, свободные от (w,r) перекрытий. Доказано, что некоторые коды являются оптимальными. Способ построения таких кодов не является новым и основан на использовании комбинаторных блок схем. Метод доказательства оптимальности таких кодов использует новый подход, использующий идеи из теории кодирования. Мне представляется, что дальнейшее развитие этого подхода является перспективным и позволит продвинутся в исследованиях свойств кодов, свободных от (w,r) перекрытий. Также доказывается единственность некоторых из этих кодов. Здесь также используются известные свойства комбинаторных блок схем. Предложен новый метод получения верхней границы на скорость кодов, свободных от (w,r) перекрытий. Для этого вводится композиционное расстояние, позволяющее применить подход получения верхних границ на мощность кода из теории кодирования. Данная верхняя граница является наилучшей из известных на сегодняшний день. Также доказываются интересные результаты для тривиальных кодов, свободных от перекрытий. Кроме того, в данной главе изучаются коды с ограничениями на возможные коалиции и окрашенные коды, свободные от перекрытий. В четвертой главе решалась задача определения метрической размерности недвоичного пространства Хэмминга. Основным результатом главы является доказательство асимптотического равенства для метрической размерности. Таким образом, задача определения метрической размерности недвоичного пространства Хэмминга для случаев $q=3$ и $q=4$ полностью решена. Кроме того, доказывается, что для задачи поиска только одного, из d дефектных элементов, суммирующая модель не дает преимущества по сравнению с классической моделью. Как я уже отмечал выше, задачи нахождения только одного элемента мне представляются крайне интересными.

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. Кроме того, предложен новый метод исправления ошибок для q-ичного канала с безошибочной обратной связью. Впервые введено понятие композиционного расстояния и получена граница на скорость кодов с таким композиционным расстоянием. Предложен новый алгоритм поиска для канала множественного доступа с двумя входами, позволяющий получить оптимальную константу при главном члене для общего числа пользователей. Таким образом, задача разработки новых методов получения более точных оценок характеристик некоторых кодов, используемых для передачи и защиты информации, в том числе обслуживающих некоторые КМД решена. Для задачи Улама предложен новый подход с точки зрения КМД, позволяющий обобщить результаты Берлекампа на q-ичный случай (q>2).
Для дизъюнктивной модели введено композиционное расстояние, позволяющее применить подход из теории кодирования и КМД для получения более точных верхних границ для скорости кодов, свободных от (w,r) перекрытий. Использование этих новых подходов позволило получить новые результаты, описанные выше.

Все результаты диссертации являются новыми. В работе даны полные, математически корректные доказательства. Практическая ценность полученных результатов определяется тем, что они могут применяться в дальнейших исследованиях в области теории кодирования, криптографии и комбинаторного поиска. Также результаты работы могут быть использованы в разных практических областях: в практической криптографии, медицине, биологии и др.
Положения и выводы, сформулированные в диссертации, получили квалифицированную апробацию на международных и российских научных конференциях и семинарах. Достоверность также подтверждается публикациями результатов исследования в рецензируемых научных изданиях, в том числе, рекомендованных ВАК.
Автореферат в целом хорошо отражает содержание диссертации.

В диссертации имеются грамматические ошибки и опечатки, затрудняющие ее чтение. Также, на мой взгляд, стоило дать более подробный литературный обзор главы 2. Некоторые результаты исследований дизъюнктивных кодов заслуживают более полного их изложения.

Отмеченные выше недостатки не снижают научную ценность работы.

Диссертация 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 всем требованиям, предъявляемым ВАК к докторским диссертациям. Ее автор В.С. Лебедев безусловно заслуживает присуждения ему ученой степени доктора физико-математических наук по указанной специальности.

9.09.2021

Официальный оппонент
доктор физико-математических наук,
профессор кафедры теории вероятностей
механико-математического факультета
Московского государственного университета
имени М.В.Ломоносова

Дьячков
Аркадий Георгиевич

Подпись А.Г. Дьячкова
заверяю
декан механико-математического факультета МГУ

(А.И. Шафаревич)

Сведения об оппоненте: Дьячков Аркадий Георгиевич гражданин РФ, доктор физико-математических наук по специальности 01.01.05 – Теория вероятностей и математическая статистика, профессор кафедры теории вероятностей механико-математического факультета ФГБОУ ВО Московского государственного университета имени М.В. Ломоносова.
Адрес: Ленинские горы, 1, Москва, 119234
Е-мэйл: agd-msu@yandex.ru
Телефон: 8 4959391403