ОТЗЫВ

на автореферат 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, позволяющих на основании комбинаторного подхода получать более точные оценки характеристик некоторых кодов, используемых для передачи и защиты информации. Описание рассматриваемых задач и предложенные решения, изложенные в автореферате, позволяют адекватно оценить выполненную работу, ее результаты и их значимость.

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.

Основные результаты диссертации:

1. Предложен алгоритм передачи информации по q-ичному каналу с безошибочной обратной связью, который является оптимальным для доли ошибок в канале, большей 1/q. Использование такого алгоритма очевидно позволит максимально эффективно использовать пропускную способность канала с заданными свойствами.

2. Предложен алгоритм поиска двух дефектных элементов, позволяющий получить оптимальную константу при главном члене асимптотики для общего числа элементов. Успех в разработке такого алгоритма позволяет рассчитывать на дальнейшее продвижение в этом направлении и разработку алгоритмов для поиска трех и более дефектных элементов.

3. Построены коды, свободные от перекрытий, и доказана оптимальность и единственность некоторых из них. Построение таких кодов, безусловно актуально для решения криптографических задач связанных с распределением ключей в коалициях.

4. Получена верхняя граница на скорость кодов, свободных от перекрытий.

5. Решена задача определения метрической размерности недвоичного пространства Хэмминга для случаев q=3 и q=4 , что позволило существенно продвинуться в решении общей задачи определения размерности.

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.

Научная новизна работы состоит в том, что в ней впервые предложен комбинаторный подход рассмотрения задач поиска 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.

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.

Обоснованность и достоверность результатов и выводов

Все результаты обоснованы строгими математическими доказательствами. Положения и выводы, сформулированные и представленные в автореферате, получили квалифицированную апробацию на международных и российских научных конференциях и семинарах.

Автореферат правильно отражает содержание диссертации, однако имеются следующие недостатки:

- Из приведенного на стр.9 описания задачи Станислава Улама неясно, что понимается под недвоичным случаем ($q>2$).
- Из описания на странице 15 неясно, почему длина информационной последовательности равна $n-(r+1)t$, это косвенно поясняется только на стр. 16.
- К сожалению, по-видимому, ограниченный объем автореферата, не позволил автору привести заявленный автором алгоритм поиска двух дефектных элементов.
- На странице 18 речь идет о решении задачи поиска активных пользователей «Во втором разделе второй главы изучается задача нахождения одного из нескольких активных пользователей» однако, к сожалению, не приводится результат решения этой задачи, так как далее автор пишет о дефектных элементах.

Однако, отмеченные выше недостатки не снижают научную ценность работы.

Судя по автореферату, работа в полной мере соответствует 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.

доктор технических наук,
заведующий кафедрой технологий
защиты информации Санкт Петербургского
государственного университета
аэрокосмического приборостроения — Беззатеев Сергей Валентинович

14.09.2021

Подпись С.В. Беззатеева
удостоверяю

Подпись работника ГУАП С.В. Беззатеева
Заверяю
Начальник отдела кадров работников
Р.П. Жилина
20__ г.

Сведения об оппоненте: Беззатеев Сергей Валентинович, гражданин РФ, доктор технических наук по специальности 05.13.01 - Системный анализ, управление и обработка информации, заведующий кафедрой технологий защиты информации Санкт Петербургского государственного университета аэрокосмического приборостроения
Адрес: Большая Морская ул., 67, Санкт Петербург, 190000
Е-мэйл: bsv@aanet.ru
Телефон: 8 8124947077