«Утверждаю»
ВРИО Директора Федерального
государственного бюджетного учреждения науки
«Институт вычислительных технологий
Сибирского отделения Российской академии наук»

_____ А.В. Юрченко

«22» _____ 2017 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

на диссертационную работу **Воробьева Ильи Викторовича**
«Разделяющие коды»,
представленную на соискание ученой степени кандидата
физико-математических наук по специальности
01.01.05 – «теория вероятностей и математическая статистика».

Представленная диссертационная работа посвящена разделяющим кодам, а также различным обобщениям дизъюнктивных кодов. Главной задачей является построение новых верхних и нижних оценок асимптотических скоростей данных кодов.

Двоичные разделяющие коды были впервые введены Ю.Л. Сагаловичем в 1965 году для решения задач, возникающих в теории автоматов. Из более новых приложений отметим разработанные в статье Д. Боне и Д. Шоу 1998-го года методы использования разделяющих кодов для защиты авторских прав на цифровую продукцию. В различное время данной тематикой занимались такие специалисты, как А.М. Барг, Р. Грэхэм, Г.А. Кабатянски, Дж. Кернер, Ж. Коэн, М.С. Пинскер, Ю.Л. Сагалович, В.М. Сидельников, Г. Симоньи, Дж. Стаддон, Д. Стинсон, Дж. Ульман, Г. Шаатун.

Диссертация состоит из введения, четырех глав и заключения. Во вводной части приводится обзор литературы по рассматриваемым задачам и излагается краткое содержание представленной работы.

В первой главе доказываются новые нижние и верхние оценки для асимптотической скорости разделяющих кодов. Двоичным разделяющим (s, l)-кодом называется двоичная матрица, у которой для любых двух наборов столбцов S и L мощности s и l, найдется строка, содержащая только нули на пересечении со столбцами из S и только единицы на пересечении со столбцами из L, или строка, содержащая только нули на пересечении со столбцами из L и только единицы на пересечении со столбцами из S. Эти коды имеют естественное обобщение на q-ичный случай.

С помощью вероятностного метода получена новая нижняя граница q-ичных разделяющих (s, l)-кодов при $s \to \infty$ и фиксированных значениях параметров l и q. Эта оценка обобщает оценку для случая $l = 1$, полученную Ч. Шенгуэном и др. в 2014 году. Для доказательства верхних границ были установлены неравенства, связывающие скорости разделяющих кодов с разными параметрами и размером алфавита q, а также неравенства, связывающие скорости разделяющих кодов со скоростями свободных от перекрытий кодов и полностью разделяющих кодов.

Полученные результаты улучшают многие ранее известные границы как в двоичном, так и в q-ичном случае.

Во второй главе диссертации рассматриваются дизъюнктивные коды со списочным декодированием. Дизъюнктивным кодом со списочным декодированием силы s и длиной списка L называется двоичная матрица, у которой для любых двух наборов столбцов S и L мощности s и L, найдется строка, содержащая только нули на пересечении со столбцами из S и хотя бы одну единицу на пересечении со столбцами из L. При длине списка $L = 1$ это определение превращается в определение классического дизъюнктивного кода. Главным результатом этой главы является доказательство новой верхней границы скоростей списочных дизъюнктивных кодов, улучшающей ранее известные границы при $L > 1$ и совпадающей с границей А.Г. Дьячкова и В.В. Рыкова для дизъюнктивных кодов при $L = 1$.

В третьей главе представленной работы исследуются почти дизъюнктивные коды. Для почти дизъюнктивных кодов допускается существование наборов из s столбцов, для которых не выполняется свойство дизъюнктивного кода, но их доля ограничена некой величиной ε, называемой вероятностью ошибки. Пропускной способностью называется точная верхняя грань скорости почти дизъюнктивных кодов при стремящейся к нулю вероятности ошибки. В диссертации методом случайного кодирования на ансамбле равновесных кодов получена нижняя оценка пропускной способности почти дизъюнктивных кодов, которая отличается от верхней в константу раз.

В четвертой главе автором исследуются многоступенчатые алгоритмы поиска дефектов с помощью специального вида тестов – групповых проверок. Анализируется ситуация, когда общее число объектов t и число тестов N стремятся к бесконечности, а число дефектов ограничено константой s, при этом требуется максимизировать скорость поиска $R \sim \log_2 t / N$. Диссертант рассматривает адаптивные многоступенчатые процедуры поиска, где N проверок разбиты на конечное (не зависящее от t и N) число ступеней p, проверки внутри которых могут зависеть от результатов проверок предыдущих ступеней. Автор решает задачу явного построения алгоритма поиска дефектов с ненулевой асимптотической скоростью. Для случая $s = 2$ приводится двухступенчатый алгоритм поиска, чья скорость совпадает со скоростью адаптивного алгоритма. Для случая произвольного s построен алгоритм, состоящий из $2s - 1$ ступени и имеющий скорость $R \geq 1 / (2s - 1)$, которая отличается от известной верхней границы скорости менее чем в два раза.

Диссертационная работа имеет непринципиальные недостатки:

1. В доказательстве третьего утверждения теоремы 2.3.1 опущено обоснование формулы 2.5.25 в виду того, что оно аналогично рассуждению из теоремы 2.2.1. Аналогичность доказательства не так очевидна, его следовало бы привести.
2. Для облегчения понимания предлагаемых в главе 4 алгоритмов поиска следовало бы привести пример их применения для малых значений общего числа объектов t.
3. В главе 4 приводятся таблицы, где количество тестов, необходимое для поиска с помощью предлагаемых алгоритмов, сравнивается с теоретико-информационной нижней границей числа тестов. Было бы интересно увидеть сравнение с количеством тестов, которое дают другие известные конструкции, например, конструкции для дизъюнктивных и списочных дизъюнктивных кодов.

Указанные замечания не снижают общего положительного впечатления о работе.

Результаты диссертации являются новыми, они интересны и важны для комбинаторной теории кодирования. Автор продемонстрировал высокий уровень владения различными вероятностными, комбинаторными и аналитическими методами.

Результаты диссертационной работы ясно изложены и снабжены подробными доказательствами.

Результаты диссертации, выносимые на защиту, опубликованы в 13 работах, 5 из которых в журналах из перечня ВАК, прошли апробацию на ряде международных конференций. Автореферат адекватно отражает содержание диссертации.

Диссертационная работа «Разделяющие коды» Воробьева Ильи Викторовича является завершенным научным исследованием и удовлетворяет всем требованиям «Положения о порядке присуждения ученых степеней» Высшей аттестационной комиссии Министерства образования и науки Российской Федерации, а ее автор, Воробьев Илья Викторович, заслуживает присуждения ему ученой степени кандидата физико-математических наук по специальности 01.01.05 (теория вероятностей и математическая статистика).

Отзыв обсужден и одобрен на заседании лаборатории информационных систем и защиты информации ФГБУН «Институт вычислительных технологий Сибирского отделения Российской академии наук» 20 февраля 2017 года (протокол № 5).

Главный научный сотрудник
лаборатории информационных систем и защиты информации
отдела информационных технологий и проблем мониторинга,
доктор технических наук

Рябко Борис Яковлевич

630090, Новосибирск, пр. Академика Лаврентьева, 6
тел.: +7(383)334-91-24,
e-mail: boris@ryabko.net

Главный научный сотрудник
лаборатории анализа и оптимизации нелинейных систем
отдел вычислительных технологий,
доктор физико-математических наук

Чубаров Леонид Борисович

630090, Новосибирск, пр. Академика Лаврентьева, 6
тел.: +7(383)333-18-82,
e-mail: chubarov@ict.nsc.ru