

Отзыв официального оппонента о диссертации И.В. Воробьева
«Разделяющие коды»,
представленной на соискание ученой степени кандидата
физико-математических наук по специальности 01.01.05 —
теория вероятностей и математическая статистика

В диссертации И.В. Воробьева рассматриваются вопросы, связанные с разделяющими кодами. Более точно, в работе рассматриваются полностью разделяющие, свободные от перекрытий и дизъюнктивные коды, а также изучается задача поиска дефектов с помощью групповых проверок.

Двоичные разделяющие коды были впервые введены и исследованы Ю.Л. Сагаловичем и А. Фридманом; q -ичные разделяющие коды были впервые рассмотрены в совместной работе М.С. Пинскера и Ю.Л. Сагаловича. Этими авторами получены различные оценки скоростей разделяющих кодов. Оцениванию скоростей разделяющих кодов были посвящены работы и многих других авторов. Такой интерес связан с несомненной актуальностью темы — разделяющие коды оказываются полезны в задаче защиты авторских прав и в некоторых криптографических задачах, связанных с распределением ключей. Дизъюнктивные коды, являющиеся частным случаем кодов, свободных от перекрытий, введенные У. Каутсом и Р. Синглтоном, также имеют множество приложений, среди которых можно выделить задачу группового тестирования. А.Г. Дьячков и В.В. Рыков ввели понятие дизъюнктивного кода со списочным декодированием, которое удалось использовать при передаче информации через канал множественного доступа в системе связи АЛОХА. Почти дизъюнктивные коды были определены Э. Макулой и др., они являются вероятностным обобщением понятия дизъюнктивных кодов.

В диссертации получены новые асимптотические оценки скоростей разделяющих кодов и списочных дизъюнктивных кодов. Стоит отметить, что И.В. Воробьев получил первую оценку снизу пропускной способности почти дизъюнктивных кодов, построил первый алгоритм поиска двух дефектов с конечным числом ступеней, достигающий информационной границы, и первый алгоритм поиска произвольного числа дефектов с конечным числом ступеней и ненулевой скоростью.

Диссертация состоит из введения и четырех глав. В первой главе речь идет о разделяющих кодах: даны основные определения, указаны приложения разделяющих кодов и сформулированы и доказаны новые теоремы. Основными результатами этой главы являются новые оценки асимптотических скоростей разделяющих кодов. Отметим, что для доказательства теоремы, содержащей оценку снизу скорости q -ичного разделяющего кода, использовался вероятностный метод. Вторая глава посвящена верхним границам асимптотических скоростей классических дизъюнктивных кодов и дизъюнктивных кодов со списочным декодированием. В третьей главе исследуется пропускная способность почти дизъюнктивных кодов. В четвертой главе обсуждается задача многоступенчатого поиска дефектов. Отметим, что результаты четвертой главы основаны на применении теории гиперграфов, на языке которых удается переформулировать задачу поиска дефектов.

Результаты, полученные в диссертации, являются новыми. Достоверность научных положений, выводов и заключений, сформулированных в диссертации, подтверждается строгими и четкими математическими доказательствами, разобранными примерами, показывающими область применения полученных результатов и их оптимальность.

Диссертационная работа носит теоретический характер. Ее результаты могут быть использованы в теории информации и в комбинаторной теории кодирования.

Работа написана на хорошем математическом уровне. Отметим, что автор для получения результатов применил различные математические методы, и одним из основных является вероятностный метод. В этой связи хочется подчеркнуть умелое владение автором методами комбинаторной теории кодирования и теории вероятностей. В то же время, в работе замечены и следующие недостатки.

1. Определения одного и того же понятия на стр. 3 во введении и на стр. 22 первой главы отличаются. Стоило бы во избежание замешательства дать одинаковые определения или объяснить, почему они эквивалентны.
2. На стр. 4 ссылку [42] лучше было бы дать там, где впервые встречается $\bar{R}(\delta)$, а на стр. 5 повторное определение этого понятия можно было бы убрать. Обозначение N_s , пожалуй, выбрано не очень удачно, из-за того, что возникает путаница с параметром s этой величины.
3. На стр. 7 в строке 3 следовало бы пояснить, почему оценка является очевидной. Кроме того, совершенно не ясно, в каком смысле она является случайной.
4. Во введении не хватает некоторого более явного сравнения известных оценок рассматриваемых величин.
5. На мой взгляд, стоило бы немного изменить структуру некоторых глав, чтобы таблицы шли сразу после результатов, из которых они следуют, — так было бы удобнее читателю.
6. На странице 24 сказано, что предположение $s \geq \ell$ сделано в силу того, что три понятия из определения 1.3.3 симметричны относительно s и ℓ , что неверно для третьего понятия. Думаю, что автор имел в виду симметричность исследуемых для этих понятий величин.
7. На странице 25 после предложения 1.3.4 не пояснено, где оно было впервые доказано. Сказано, что в работе [10] рассмотрен только случай (2,1)-кодов. На той же странице впервые встречается понятие каскадного кода, стоило заранее дать определение.
8. На странице 37 и далее встречается неопределенное ранее понятие “объем”, для которого в предыдущей главе использовалось слово “мощность”.
9. Замечен ряд опечаток нематематического характера (стр. 1 строка 6; стр. 15 строка 3; стр. 17 строки 1 и 3; стр. 25 строки 16 сверху и 6 снизу; стр. 30 строка 11 снизу; стр. 32 строка 13; стр. 33 строка 4 снизу; стр. 36 строки 6 и 9; стр. 40 строка 5 снизу;

стр. 43 строка 14 снизу; стр. 48 строка 11; стр. 50 строка 7; стр. 55 строка 5 снизу;
стр. 56 строка 10 снизу; стр. 67 строка 14).

Указанные недостатки относятся лишь к представлению материала в диссертации, а не к ее математической стороне, и не снижают общего положительного впечатления от работы (как и не снижают впечатления, что работа написана очень аккуратно). Работа апробирована на различных представительных семинарах и научных конференциях; ее результаты адекватно и полно отражены в 13 печатных работах, из них 5 статей в рецензируемых журналах (все входят в перечень ВАК) и 8 тезисов докладов в рецензируемых трудах международных конференций. Основное содержание диссертации своевременно и полно опубликовано в открытой печати. Автореферат правильно отражает содержание диссертации.

Диссертация является научно-квалификационной работой, результаты которой вносят весомый вклад в комбинаторную теорию кодирования. Она соответствует критериям, установленным Положением о порядке присуждения ученых степеней, утвержденным Постановлением Правительства Российской Федерации №842 от 24 сентября 2013 года, а ее автор Воробьев Илья Викторович заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 01.01.05 — Теория вероятностей и математическая статистика.

Кандидат физико-математических наук
по специальности 01.01.05 — Теория
вероятностей и математическая статистика,
доцент кафедры дискретной математики

Жуковский Максим Евгеньевич

22 марта 2017 года

Адрес электронной почты: zhukmax@gmail.com.

Телефон: (495)4084554.

Организация — место работы: ФГАОУ ВО «Московский физико-технический институт (государственный университет)».

Адрес организации: 141701, г. Долгопрудный Московской обл., Институский пер., 9.

Адрес официального сайта организации: www.mipt.ru.

Должность: доцент.

Подпись к.ф.-м.н. М.Е. Жуковского заверяю



к.ф.-м.н.

н., доцент Скалько Юрий Иванович

ученый секретарь МФТИ