Отзыв официального оппонента на диссертацию Воробьева И.В.

«Разделяющие коды»,

представленной на соискание ученой степени кандидата физико-математических наук

по специальности 01.01.05 – Теория вероятностей и математическая статистика.

Диссертационная работа И.В.Воробьева посвящена исследованию довольно широкого класса вероятностно-комбинаторных задач, возникших независимо в теории информации в теории планирования эксперимента. Пожалуй, наиболее известной в математике является задача о дизъюнктивных кодах, которая приобрела популярность благодаря статье П.Эрдеша с соавторами, название которой и является постановкой задачи - «Системы множеств, в которых ни одно из них не покрывается объединением двух других» (1982.) Замечу, что одновременно в работе руководителя диссертанта профессора А.Г. Дьячкова (совместно с В.В.Рыковым) для этой же задачи были получены не только несколько более сильные результаты, но и в более общем случае. В дальнейшем были придуманы различные обобщения этой задачи, все в той или иной степени использующие понятие разделимости множеств векторов, и одновременно интерес к этим задачам возрастал со стороны практики, особенно после того, как эти коды нашли применение при защите авторских прав. Поэтому тема диссертационной работы несомненно является актуальной.

Перейдем теперь к изложению основных научных результатов, оценке их новизны и значимости для науки. Отмечу, что диссертация, несмотря на ее довольно обычный объем (74 стр. текста без учета литературы), в какой-то мере переполнена результатами. Это, несомненно, не недостаток, однако не позволяет уделить всем полученным результатам достаточное внимание в отзыве. Поэтому я ограничусь рассмотрением только наиболее важных, с моей точки зрения, результатов.

В первой главе исследуются разделяющие коды, а также родственные классы кодов, такие как полностью разделяющие коды и коды, свободные от перекрытий. Довольно общая концепция разделяющих кодов формально впервые появилась в работе Д.Стинсона около 20 лет назад, но важным является не столько дать общее определение, собирающее под одну крышу довольно разнородные математические объекты, сколько выделение схожих классов объектов, в данном случае – кодов, и их совместное исследование. Эта задача во многом решается именно в первой главе. Напомню некоторые определения. Множество q-ичных слов фиксированной длины n называется (s,l)-разделяющим кодом, если для любых двух его непересекающихся подмножеств, мощности не более s и l соответственно, существует *разделяющая* их координата i, т.е. такая, что значения слов в этой координате данных двух подмножеств не пересекаются. Диссертанта интересуют такие коды с максимально возможным числом слов, которое я обозначу через D(s,l;n|q). Давно известно, что величина D растет экспоненциально с ростом длины кода, при фиксированных остальных трех параметрах, но показатель этой экспоненты, называемый *скоростью кода*, не только неизвестен, но неизвестен даже его порядок, например, при больших s, но фиксированном l (размер алфавита q мы считаем фиксированным, если не оговорено обратное). Более того, достаточно хорошие верхние и нижние границы на скорость максимального разделяющего кода были известны только в двоичном случае. Автор диссертации установил ряд таких верхних границ на скорость разделяющих кодов, теоремы 1.4.1 и 1.5.1, что позволило ему найти новую верхнюю границу на скорость (s, s)-разделяющих кодов, показывающую, что скорость таких кодов ограничена сверху O(2^{-2s}), т.е. экспоненциально мала по s, что довольно неожиданно. По существу, полученная верхняя граница основывается на аналоге классической границы Плоткина в теории кодирования (или границы Рэнкина в дискретной евклидовой геометрии), которая доказывается для разделяющего «расстояния» в лемме 1.7.1. Отношение верхней и нижней границ сравнительно невелико -- имеет порядок log s при фиксированном l и q, при этом остается неясным, что надо улучшать в предложенных методах для того, чтобы сблизить границы – пытаться улучшить верхние границы, обобщая метод линейного программирования на данную задачу, что, впрочем, может оказаться довольно сложной задачей, либо пытаться улучшить нижнюю границу, выбирая более специальный ансамбль кодов. Особо отмечу, что развитый в первой главе аппарат работает, как для разделяющих кодов, так и для их модификаций – полностью разделяющих кодов, дизъю-

нктивных кодов и кодов, свободных от перекрытий. Основное содержание второй главы – это результаты об асимптотике дизъюнктивных кодов со списочным декодированием. Одним из интересных результатов является доказательство того, что если объем списка L ограничен сверху, а параметр s стремится к бесконечности, то ослабление условия дизъюнктивности кода до «списочности» дает выигрыш в скорости не более чем в L раз. В параграфе 2.4 рассматриваются так называемые планы дизъюнктивного поиска. На самом деле, это сигнатурные коды для дизъюнктивного канала множественного доступа, и в рамках данной диссертации было бы более естественно рассматривать их именно так

В третьей главе рассматриваются почти дизъюнктивные коды, т.е. коды, у которых доля подмножеств, для которых не выполнено свойство дизъюнктивности, стремится к нулю с ростом длины кода. Диссертант доказывает, что скорость наилучших почти дизъюнктивных кодов при больших s асимптотически не меньше чем ln2 /s, что дает порядок скорости таких кодов, так как верхняя граница говорит, что скорость не больше чем 1/s. Представляется очень интересным найти точное значение скорости лучших почти дизъюнктивных кодов при больших s и сравнить с известным результатом М.Б.Малютова и В.Л.Фрейдлиной (1973), доказавших, что пропускная способность дизъюнктивного канала равна 1/s.

Последняя, четвертая глава посвящена многошаговым алгоритмам нахождения дефектов. Рассмотренные в предыдущих главах диссертации разделяющие коды можно рассматривать как одношаговые, т.е. детерминированные, алгоритмы поиска дефектов. Изучались также и многошаговые алгоритмы, или алгоритмы с обучением, что соответствует передаче сообщений по соответствующему каналу с бесшумной мгновенной обратной связью. И если для обычных каналов связи, как например дискретный канал с независимыми ошибками, соответствующая теорема Шеннона говорит, что обратная связь не увеличивает пропускную способность канала, то это неверно для рассматриваемых каналов с множественным доступом. Самым интересным результатом этой главы является теорема 4.3.1, устанавливающая точное значение скорости для поиска двух дефектов четырехшаговым алгоритмом, а именно, 1/2.

Все полученные в диссертации результаты являются новыми, впервые полученными автором. Их достоверность и обоснованность основывается на корректном использовании математического аппарата, включая методы и результаты теории вероятностей. Достоверн ость результатов диссертации подтверждается многократными выступлениями диссертант а на научных семинарах и представительных международных конференциях. Основные р езультаты диссертации полностью отражены в 13 опубликованных работах, из них 5 – пу бликации в журналах из перечня ВАК. Автореферат правильно и полно отражает содерж ание диссертации, которое соответствует паспорту специальности 01.01.05 – теория вероя тностей и математическая статистика.

Теоретическая значимость рассматриваемой диссертации состоит в довольно полном и скрупулезном исследовании разделяющих и родственных к ним кодов методами теории вероятностей и комбинаторики. Практическая ценность диссертации основывается на применении разделяющих кодов для защиты авторских прав на цифровой контент, и применении дизъюнктивных кодов в планировании экспериментов.

Замечания к диссертации носят стилистический характер. Так, мне не нравится стиль изложения диссертации, когда сначала формулируются все теоремы главы, а потом отдельно идут их доказательства, тоже все вместе. Я бы предпочел традиционное изло-жение: формулировка результата, его доказательство и, если уместно, обсуждение. Кроме того, имеются неудачные названия. Например, для дизъюнктивных кодов со списочным декодированием никакое списочное декодирование на самом деле не рассматривается, а имеется в виду только то, что список соответствующих слов не может быть больше заданного порога. Лучше было бы придерживаться принятой формулировки как «код, декодируемый списком фиксированного (ограниченного) объема» (В.М. Блиновский). Так же неудачная формулировка пропускной способности почти дизъюнктивных кодов, так как речь идет о максимальной скорости почти дизьюнктивных кодов, тогда как пропус кная способность - это параметр канала. Указанные замечания являются несуществен ными и не могут изменить общей положительной оценки диссертационной работы.

ЗАКЛЮЧЕНИЕ

Представленная диссертация И.В. Воробьева является законченной научно-квалификационной работой, содержащей решение научной задачи оценки параметров наилучших разделяющих и дизъюнктивных кодов, которая имеет важное значения для дальнейшего развития теории информации как части теории вероятностей. На основании всего вышеизложенного считаю, что диссертация удовлетворяет всем требованиям «Положения о присуждении ученых степеней», а ее автор, Воробьев Илья Викторович заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 01.01.05 - теория вероятностей и математическая статистика.

Официальный оппонент:
Кабатянский Григорий Анатольевич,
доктор физико-математических наук,
советник по науке ректора Сколковского института науки и технологий

Адрес: 143025, Московская область, Одинцовский район, Сколково, ул. Новая, д. 100
Телефон: +7 (985) 667-89-21
Адрес электронной почты:g.kabatyansky@skoltech.ru

Подпись Кабатянского Г.А. заверяю

Менеджер по административным и кадровым вопросам
Сколковского Института науки и технологии
Коновалова Л.Б.

«22» марта 2017 г.