ОТЗЫВ

научного руководителя о диссертации
Полянского Никиты Андреевича
«Коды, свободные от перекрытий» (Cover-Free Codes),
представленной на соискание ученой степени кандидата
физико - математических наук по специальности
01.01.05 - «теория вероятностей и математическая статистика».

Мотивируемое широким кругом приложений понятие *свободного от перекрытий* (s,ℓ)-кода (СП (s,ℓ)-код) длины N и объема t можно интерпретировать как двоичную $(N\times t)$-матрицу инцидентности семейства множеств, состоящего из t подмножеств конечного N-множества, для которого пересечение любых ℓ, $1\le\ell<t$, членов семейства подмножеств не покрывается объединением (не принадлежит объединению) любых других s, $1\le s<t$, членов семейства. Основные математические результаты в теории СП (s,ℓ)-кодов связаны с исследованием логарифмической асимптотики $(N\to\infty)$ максимального объема $t(s,\ell,N)$ таких кодов длины N, т.е. с построением верхних и нижних границ для функции целочисленных параметров $s,\ell=1,2,\ldots$:

$$R(s,\ell)\triangleq\varlimsup_{N\to\infty}\frac{\log_2 t(s,\ell,N)}{N},$$

называемой, следуя традиции комбинаторной теории кодирования, *скоростью* СП (s,ℓ)-кодов. Отметим, что при $s,\ell\ge 2$ СП (s,ℓ)-коды были предложены в 1988 году К. Митчеллом и Ф. Пайпером для решения задачи распределения шифровальных ключей между пользователями криптографических сетей.

В наиболее важном для приложений частном случае $\ell=1$ определение СП $(s,1)$-кода, которое было введено в 1964 году У. Каутсом и Р. Синглтоном как *дизъюнктивного s-кода* (ДК), означает, что объединение любых s членов семейства покрывает те и только те члены семейства, из которых составлено это объединение. В основополагающей статье 1964 года были разработаны комбинаторные и алгебраические методы классической теории кодов, исправляющих ошибки, для применения к анализу конструкций ДК. Задача получения границ максимального объема $t(s,1,N)$ дизъюнктивных s-кодов длины N оставалась открытой до 1982 года, когда мне совместно с В.В. Рыковым, используя важное свойство ДК, обнаруженное в 1975 году Л.А. Бассалыго, удалось найти наилучшую к настоящему времени *верхнюю* границу для скорости $R(s,1)$.

В 1989 году я построил наилучшую к настоящему времени *нижнюю* границу скорости $R(s,1)$, основанную на технике оценивания вероятностей больших уклонений в методе случайного кодирования для ансамбля кодов, в котором слова выбираются независимо с равномерным распределением из множества, состоящего из всех $\binom{N}{w}$ двоичных слов длины N и веса w, $1\le w\le N$. В методе случайного кодирования для такого ансамбля, называемого *равновесным* ансамблем, логарифмическая асимптотика вероятностей больших уклонений вычисляется существенно сложнее, чем для ансамбля с *независимыми компонентами*

кодовых слов, где можно применять более простые методы оценивания логарифмической асимптотики, но получать при этом менее точные нижние оценки скорости $R(s,1)$, являющейся основной комбинаторной характеристикой оптимальных дизъюнктивных s-кодов.

Для общего случая СП (s,ℓ)-кодов, $2 \le \ell \le s$, наилучшие к настоящему времени верхняя и нижняя границы скорости $R(s,\ell)$ были построены мной совместно с П.А.Виленкиным в 2002 году. При этом нижняя граница для $R(s,\ell)$ в 2002 году была доказана с помощью ансамбля кодов с независимыми компонентами и с тех пор регулярно предлагаемая мной многим ученикам задача ее улучшения за счет применения равновесного ансамбля оставалась нерешенной.

Диссертация Н.А. Полянского состоит из введения и 3 глав и изучает ряд актуальных для приложений задач комбинаторной теории кодирования и теории информации для кодов, свободных от перекрытий. Целью **первой главы** диссертации является давно ожидаемое мной от учеников построение нижней границы скорости $R(s,\ell)$ как границы случайного кодирования для ансамбля равновесных кодов. С этой задачей Н.А. Полянский успешно справился, существенно обобщив аналитическую технику анализа вероятностей больших уклонений, которая у меня в 1989 году была лишь для частного случая $\ell = 1$. Для всех фиксированных значений параметров $2 \le \ell \le s$ он улучшил численные значения нижней границы скорости $R(s,\ell)$, полученной мною и П.А. Виленкиным в 2002 году, и кроме того, показал что асимптотика (ℓ=const, $s \to \infty$) границы случайного кодирования для равновесного ансамбля двоичных кодов не меняется по сравнению с ансамблем с независимыми компонентами. Также заслуживающим внимания, хотя и не основным материалом первой главы, мне представляется обобщение известных конструкций ДК на случай кодов, свободных от перекрытий.

Во **второй главе** диссертации автор предлагает дальнейшую разработку задачи в теории кодов, свободных от перекрытий, когда такие коды используются для стандартного описания N статическом проверок при планировании отсеивающих экспериментов в предложенной Д. Торни в 2000 году для приложений молекулярной биологии и математически описанной мной и П.А. Виленкиным в 2002 году комбинаторной дизъюнктивной модели неадаптивного поиска неизвестного супермножества (скрытого (s,ℓ)-гиперграфа), о котором лишь известно, что это супермножество состоит из не более s дефектных подмножеств t-множества, где дефектные подмножества t-множества не покрывают друг друга и каждое из них имеет объем не превосходящий ℓ. Принципиально новым продвижением Н.А. Полянского является теоретико-информационный подход когда при $N \to \infty$ допускается стремящаяся к нулю вероятность ошибки решения, принимаемого по результатам всех N проверок. В такой постановке вместо характеристики скорости кода $R(s,\ell)$ с нулевой ошибкой критерием соответствующего кода является аналог шенноновской пропускной способности $C(s,\ell)$, где $C(s,\ell) \ge R(s,\ell)$. Отмечу, что для частного случая $\ell = 1$ нетривиальный результат по вычислению пропускной способности $C(s,1) = 1/s$ был получен в 1978 году М.Б. Малютовым и В.Л. Фрейдлиной. Основными достижениями диссертанта в этой главе являются выводы нетривиальных нижней границы для пропускной способности $C(s,\ell)$ (прямая теорема Шеннона) и верхней границы пропускной способности $C(s,\ell)$ (обратная теорема Шеннона) которые, как устанавливает автор, по порядку асимптотики (ℓ=const, $s \to \infty$) отличаются от известных нижних и верхних границ комбинаторной скорости $R(s,\ell)$. Для вывода нижней границы применяется метод случайного кодирования из первой главы диссертации для ансамбля равновесных кодов. Для получения верхней границы приходится существенно развивать разработанную в 2003 году В.С. Лебедевым технику

доказательства обобщенной границы Плоткина скорости кода $R(s,\ell)$ с нулевой ошибкой.

Третья глава диссертации Н.А. Полянского посвящена двум задачам адаптивного поиска скрытого гиперграфа, для которых автору удается построить оптимальные адаптивные алгоритмы поиска, скорость или пропускная способность которых достигает очевидную верхнюю границу $1/(s\,\ell)$. Первая задача формулируется как полностью адаптивный поиск, для которого к настоящему времени была достигнута лишь нижняя граница скорости $1/(2s\,\ell)$. Вторую предложенную самим диссертантом естественную задачу теории планирования отсеивающих экспериментов можно назвать вычислением пропускной способности для дизъюнктивной модели поиска скрытого гиперграфа с одной ступенью адаптивности.

Из этого перечня видно, что диссертант проявил активность как при разработке и решении актуальных для приложений асимптотических задач комбинаторной теории кодирования, так и при применении классических теоретико - вероятностных методов для вычисления асимптотики важных теоретико - информационных характеристик. При этом им проявлена большая изобретательность при решении конкретных задач, а также свободное владение различными вероятностными, комбинаторными, аналитическими и числовыми методами. Мне особенно импонировала его настойчивость при преодолению аналитических трудностей в первой главе а также самостоятельность и инициатива, показанные при работе над второй и третьей главами диссертации, при постановках и решениях задач, связанных с обобщениями классических границ скорости дизъюнктивных кодов.

Диссертация Н.А. Полянского несомненно удовлетворяет всем требованиям «Положения о порядке присуждения ученых степеней» Высшей аттестационной комиссии Министерства образования и науки Российской Федерации, а ее автор, Полянский Никита Андреевич, заслуживает присуждения ему ученой степени кандидата физико - математических наук по специальности 01.01.05 - «теория вероятностей и математическая статистика».

Научный руководитель:
доктор физико - математических наук
по специальности 01.01.05,
профессор кафедры теории вероятностей
механико-математического факультета
ФГБОУ ВО «Московский государственный
университет им. М.В. Ломоносова»
тел. +7(495)939-14-03
электронная почта: agd-msu@yandex.ru

Дьячков Аркадий Георгиевич

Подпись профессора А.Г. Дьячкова заверяю
и.о. декана механико - математического факультета МГУ,
доктор физико - математических наук,
профессор

05.05.2016 г.

Чубариков Владимир Николаевич