

ОТЗЫВ

официального оппонента на диссертационную работу Полянского Никиты Андреевича «Коды, свободные от перекрытий», представленную к защите на соискание ученой степени кандидата физико-математических наук по специальности 01.01.05 - теория вероятностей и математическая статистика.

Актуальность темы диссертации. Диссертационная работа Полянского Н.А. посвящена вопросам теории кодов, свободных от перекрытий. Свободный от перекрытий (s, l) код длины N и объема t можно определить как двоичную N на t матрицу со следующим свойством. Для любых двух наборов столбцов мощности s и l найдется строка, в которой все столбцы из первой группы имеют значение 0, а все столбцы из второй группы имеют значение 1. Основная проблема состоит в том, чтобы минимизировать число строк такой матрицы при фиксированном объеме кода.

Важнейшими приложениями свободных от перекрытий кодов являются разнообразные задачи теории комбинаторного поиска и криптографическая проблема распределения секретных ключей. Изучением этих вопросов занимались и занимаются многие математики. Таким образом, задачи, связанные со свободными от перекрытий (СП) кодами, были и продолжают быть актуальными.

Основные результаты работы и новизна. Диссертация состоит из введения, трех глав, заключения и списка литературы. Во введении обозначены основные цели работы, дан обзор литературы по исследуемым задачам и приведено краткое содержание диссертации.

Первая глава диссертации посвящена главным образом новой границе снизу для асимптотической скорости СП кодов. При выводе нижней оценки автор развивает метод случайного кодирования на равновесных кодах, ранее используемый Дьячковым А.Г., Рашадом А.М. и Рыковым В.В. (1989 год) при доказательстве аналогичных оценок для дизъюнктивных кодов. Установленная граница улучшает наилучшую ранее известную оценку, доказанную Дьячковым А.Г., Виленкиным П.А., Макула А., Торни Д. (2002 год).

Вторая глава диссертации посвящена почти свободным от перекрытий (ПСП) кодам и исследуется некоторый аналог асимптотической скорости СП кодов – пропускная способность ПСП кодов. Автор получает нижнюю границу для пропускной способности, используя аналогичные соображения,

что и в первой главе. Доказательство же верхней границы для пропускной способности ПСП кодов можно назвать развитием метода вывода обобщенной границы Плоткина из моей работы (2003 год), используемого ранее также и другими авторами для получения верхней границы и некоторого рекуррентного неравенства для асимптотической скорости СП кодов.

Третья глава диссертации посвящена алгоритмам поиска скрытого гиперграфа. Наиболее интересным результатом в данной главе является то, что получена точная равенство для асимптотической скорости адаптивного поиска скрытого гиперграфа. Таким образом был улучшен результат работы Абаси Х., Бшоути Н., Маззави Х. (2014 год).

В заключении сформулированы основные достижения работы, а также автором сформулированы некоторые направления для дальнейших исследований.

Критический анализ диссертации. К диссертации имеется следующее существенное замечание. В пятом разделе первой главы приводятся таблицы верхних границ для $N(t,3,3)$ и $N(t,4,2)$ (страницы 42-43).

В них указывается, что существуют коды, для которых $N(11,3,3)=66$, $N(12,3,3)=220$, $N(16,3,3)=560$ и $N(121,3,3)=660$. Можно существенно усилить данное утверждение.

Существуют коды, для которых $N(16,3,3)=112$, $N(22,3,3)=176$ и $N(23,3,3)=399$. Это вытекает из конструкций кодов Препараты и комбинаторных 4-(23,7,1) и 4-(27,6,1) дизайнов.

Аналогичное замечание для $N(t,4,2)$. Указано, что существуют коды, для которых $N(13,4,2)=78$ и $N(17,4,2)=136$. Но из существования комбинаторных 3-(14,4,1) и 3-(17,5,1) дизайнов вытекает существование кодов, для которых $N(13,4,2)=65$ и $N(17,4,2)=68$. Данное замечание существенно, поскольку коды на малых длинах в дальнейшем могут использоваться в каскадной конструкции.

В целом, несмотря на это замечание, оценка диссертации остается положительной.

Полнота опубликования основных результатов диссертации. Все основные результаты работы своевременно и в полном объеме опубликованы в 10 работах, в числе которых 3 статьи в журналах, включенных в перечень ведущих рецензируемых научных журналов и изданий ВАК. Основные результаты прошли апробацию на многих международных конференциях. Результаты диссертации неоднократно и подробно докладывались автором на семинаре по теории кодирования под руководством Л.А. Бассалыго в Институте Проблем Передачи Информации им. А.А. Харкевича РАН. Автореферат правильно и полно отражает содержание диссертации.

Диссертационная работа Н.А. Полянского в целом представляется законченным научным исследованием, содержащим решение ряда задач теории кодов, свободных от перекрытий. Достоверность полученных результатов не вызывает сомнений. Отмечу, что в своей диссертационной работе Н.А. Полянский существенным образом использует вероятностный метод и развивает его теоретические возможности, а результаты работы вносят вклад в развитие комбинаторной теории кодирования.

Диссертация 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».

кандидат физико-математических наук
по специальности 01.01.05 - «теория
вероятностей и математическая статистика»
должность: старший научный сотрудник
место работы: ФГБУН «Институт проблем
передачи информации им. А.А. Харкевича РАН»
адрес: 127051, г. Москва, Большой Каретный
переулок, д.19 стр. 1.
тел. (в организации): 8 (495) 650-42-25
электронная почта: lebedev37@mail.ru

Подпись
Лебедев В.С.
УДОСТОВЕРЯЮ
Зав. канцелярией *с*



*Лебедев
Владимир
Сергеевич*