Отзыв официального оппонента д.ф.-м.н., профессора Аблаева Ф.М. о диссертации Мусатова Даниила Владимировича «Комбинаторные методы в теории колмогоровской сложности с ограничением на ресурсы»

на соискание ученой степени кандидата физико-математических наукпо специальности 01.01.06 — математическая логика, алгебра и теория чисел.

В алгоритмической теории информации колмогоровская сложность объекта (слова, текста) есть мера вычислительных ресурсов, необходимых для точного определения этого объекта.

Сложность слова x определяется как длина кратчайшей программы p, печатающей слово x на пустом входе. Более общее определение — условная сложность слова x при известном y, которая равна длине кратчайшей программы, печатающей x на входе y. Условная сложность измеряет количество информации в x, отсутствующей в y. Подобно тому, как теория алгоритмов расширяется теорией сложности вычислений, теория колмогоровской сложности расширяется теорией колмогоровской сложности с ограничением на ресурсы, где программа p работает ограниченное время и использует ограниченный объём памяти. Хотя первые результаты были получены ещё в 1960-х годах, активное развитие области началось лишь в XXI веке, когда появились прорывные работы Г.Бюрмана, С.Лаплант, Т.Ли, Д. ван Мелкебеека, А.Е.Ромащенко, Л.Фортноу и других.

В диссертации Д.В.Мусатова доказано несколько новых фактов в этой области. Интерес представляют не только сами утверждения, но и методы, при помощи которых они получены. Три основных результата связаны с теоремой Ан.А. Мучника об условном кодировании. Эта теорема утверждает, что для любых слов a и b существует программа p, перерабатывающая b в a, имеющая близкую к минимальной длину (т.е., примерно равную колмогоровской сложности слова a при известном b) и при этом простая относительно a (т.е., условная сложность p при известном a мала). Понятия «близости» и «малости» понимаются как равенство с точностью до прибавления логарифмического слагаемого.

Первый основной результат, изложенный в третьей главе диссертации, заключается в новом доказательстве теоремы Мучника при помощи экстракторов. Путём небольшого изменения техники передоказано и обобщение теоремы для случая нескольких условий. Именно установление связи с теорией экстракторов позволило доказать последующие результаты.

Второй и третий результаты посвящены распространению теоремы Мучника на колмогоровскую сложность с ограничениями на память и время, соответственно. В четвёртой главе доказываются два формально несравнимых по силе аналога теоремы Мучника для колмогоровской сложности с ограничением на память. Первый аналогиспользует явные конструкции экстракторов и потому может быть усилен в будущем, если будут найдены лучшие конструкции. Второй аналог использует технику, позволяющую избежать перебора на экспоненциальной памяти без использования явных конструкций. Эта техника названа автором «наивной дерандомизацией». Идея состоит в том, чтобы заменить случайный объект на результат работы генератора псевдослучайных чисел Нисана–Вигдерсона. Для реализации этой идеи нужно выполнить несколько шагов. Во-первых,нужно сформулировать свойство, распознаваемое схемой полиномиального размера и константной глубины и такое, что объект с этим свойством годится для последующей конструкции. Во-вторых, нужно доказать, что случайный объект обладает этим свойством с отделённой от нуля вероятностью. В-третьих, нужно сделать вывод, что объекты с таким свойством встречаются среди результатов работы генератора. Наконец, в-четвёртых, нужно предъявить способ поиска аргумента генератора, на котором будет выдан нужный результат. Все шаги аккуратно разбираются автором, кроме того, доказывается и вариант теоремы для нескольких условий. В отличие от сложности без ограничений на ресурсы, для сложности с ограничением на память удаётся доказать теорему не только для полиномиального, но и для экспоненциального числа условий.

В пятой главе делается попытка переноса теоремы Мучника на колмогоровскую сложность с ограничением по времени. Непосредственный перенос наталкивается на трудности, связанные спроблемой равенства классов P и NP. Автору удаётся доказать довольно экзотический вариант теоремы для сложности с полиномиальным ограничением на время. Программа, перерабатывающая b в a за полиномиальное время, работает в т.н. модели Артура-Мерлина. Это означает, во-первых, что программа вероятностная. Во-вторых, она получает некоторую подсказку. При этом программа проверяет правильность подсказки втаком смысле: при правильной подсказке она с высокой вероятностью вернёт a, при неправильной — либо тоже a, либо символ ошибки. В доказательстве используется конструкция Бюрмана-Ли-ван Мелкебеека, которая, в свою очередь, опирается наконструкцию экстракторов Тревисана.

Наконец, в шестой главе метод «наивной дерандомизации» применяется в другой ситуации. А именно, изучаются вопросы существования колмогоровских экстракторов с ограничением на память. Понятие колмогоровского экстрактора было введено Дж. Хичкоком, А.Паваном и Н.В. Винодчандраном, которые доказали их существование. Затем теоремы существования были усилены в работах М.Зиманда. Грубо говоря, колмогоровский экстрактор — это функция, преобразующая два слово в одно, такая что если оба аргумента имеют достаточно большую сложность и не слишком большую зависимость, то значение имеет небольшой дефект случайности, т.е. разность между длиной и сложностью. В оригинальной статье было замечено, что конструкция требует полиномиальной памяти. Однако в конструкции Зиманда это было ужене так. В диссертации конструкция Зиманда модифицирована и при помощи метода «наивной дерандомизации» распространена на случай полиномиальной памяти.

Текст диссертации хорошо структурирован, написан аккуратно и чётко, все результаты снабжены подробными доказательствами. Наиболее сложные конструкции проиллюстрированы рисунками, схемами и записями алгоритмов на псевдокоде.

В работе содержитсянесколько несущественных ошибок и опечаток.
Например,

- в формулировке теоремы 2.5 на стр. 15 в правой части пропущены ограничения на время и память.
- Утверждение Теоремы 3.5 о существовании экстрактора ведется вероят-

ностным методом: для случайного графа с заданными параметрами правильно доказывается, что он обладает нужными свойствами с положительной вероятностью. В заключении доказательства (стр 44) автор пишет

... получаем, что вероятность события случайный граф НЕ является прфиксным экстрактором положительна. Значит, префиксные экстракторы существуют, ч.т.д

Понятно, что либо следует убрать отрицание "*НЕ*", либо заменить слово "*положительна*" на фразу "*меньше единицы*".

- Лемма 5.7 на стр. 86 взята из работы [13], но при этом изложенное доказательство сложнее оригинального. Остаётся неясным, была ли в исходном доказательстве какая-либо ошибка.

Указанные недостатки незначительны и не влияют на общее положительное впечатление о работе.

Диссертация является законченной научной квалификационной работой. Научные результаты диссертации, выносимые на защиту, получены лично автором, являются новыми и обоснованы строгими математическими доказательствами. Результаты других авторов, а также соавторов, упомянутые в тексте диссертации, отмечены соответствующими ссылками. Текст автореферата соответствует содержанию диссертации.

Таким образом, в диссертации получены три новых и интересных результата о колмогоровской сложности с ограничением на ресурсы. Все результаты диссертации рассказывались на семинарах и конференциях и опубликованы в 7 статьях автора, из которых 6 —в изданиях, входящих в перечень рецензируемых научных изданий ВАК Минобрнауки РФ.

Диссертация удовлетворяет всем требованиям ВАК Минобрнауки РФ, предъявляемым к диссертациям на соискание ученой степени кандидата физико-математических наук. По моему мнению, ее автор заслуживает присуждения ему ученой степени кандидата физико-математических наук по специальности 01.01.06 — математическая логика, алгебра и теория чисел.

Зав. кафедрой теоретической кибернетики ИВМиИТ КФУ
д. ф.-м. н., профессор Ф.М.Аблаев

28 января 2015 г.

ИНСТИТУТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГАОУ ВПО «КАЗАНСКИЙ (ПРИВОЛЖСКИЙ) ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Кремлевская ул., д.35, Казань, 420008
ПОДПИСЬ
Ф.М. Аблаева заверяю
Секретарь