Отзыв научного руководителя д.ф.-м.н., профессора Верещагина Н.К. о диссертации Мусатова Даниила Владимировича «Комбинаторные методы в теории колмогоровской сложности с ограничением на ресурсы» на соискание ученой степени кандидата физико-математических наук по специальности 01.01.06 — математическая логика, алгебра и теория чисел.

Колмогоровская сложность слова y при известном x определяется как длина кратчайшей программы, которая на входе x печатает (выдаёт на выход) y. Это определение было дано А.Н. Колмогоровым в его основополагающей работе «Три подхода к определению понятия "количество информации"» 1965 года. В той же работе А.Н. Колмогоров отметил, что это определение обладает одним существенным недостатком: оно не учитывает трудности переработки программы p и объекта x в объект y. Теория колмогоровской сложности, учитывающая объём ресурсов, необходимых для переработки программы в результат, стала активно развиваться лишь в XXI веке и столкнулась с серьезными трудностями, связанными с проблемой перебора. Несмотря на эти трудности, в ней было получено несколько глубоких результатов, связанных с именами Бюрмана, Лаплант, Ли, Ромащенко, Фортноу и других. Как пишет диссертант, «теория сложности с ограничением на ресурсы все еще находится в стадии накопления фактов».

Диссертация Д.В. Мусатова добавляет несколько новых, интересных и технически сложных результатов в эту «копилку фактов». Её основные результаты связаны с теоремой Андрея Мучника об условных программах. Эта теорема утверждает, что для любых слов x, y существует программа p переработки x в y почти минимальной длины (равной, напомним, колмогоровской сложности слова y при известном x) и при этом *колмогоровская сложность p при известном y мала* (то есть, программа p проста при известном y). «Почти минимальность» означает минимальность с точностью до логарифмических (от длин исходных слов) слагаемых и так же понимается «малость» условной сложности p при известном y.

Про любой интересный результат в теории колмогоровской сложности естественно возникает вопрос, в какой мере он переносится на сложность с ограничением на ресурсы. Разные результаты ведут себя по-разному в этом отношении. Например, теорема Колмогорова–Левина о сложности пары не переносится на сложность с полиномиальными ограничениями времени (если существуют односторонние функции, результат Лонгпре и Мокаса), а теорема о том, что все элементы множества малого размера и малой колмогоровской сложности сами имеют малую колмогоровскую сложность, переносится в некотором варианте, а именно, для так называемой сложности различения (Бюрман, Лаплант, Фортноу). Естественно возник вопрос от том, в какой мере результат Мучника переносится на сложность с ограничением ресурсов. Об этом спрашивали как сам Мучник, так и А. Шень, упростивший исходную конструкцию Мучника. Заметим, что в исходном доказательстве теоремы Мучника короткая программа, преобразующая y в p, выполняет перебор на экспоненциальной памяти (от длин исходных слов). Это же относится и к

самой программе p.

Этот вопрос может быть уточнён разными способами, в зависимости от того, какие ресурсы мы ограничиваем, и каким образом. В наиболее красивом результате диссертанта ограничивается память вычисления и эти ограничения полиномиальны. Этому посвящена четвертая глава диссертации. В ней доказано, что программе p достаточно памяти полиномиального размера при условии, что и кратчайшей программе преобразования x в y тоже достаточно памяти полиномиального размера (без такой оговорки утверждение попросту неверно). Кроме того, короткая программа преобразования y в p также работает на памяти полиномиального размера. Особенно интересна техника, использованная в доказательстве этого результата и позволяющая избегнуть перебора на экспоненциальной памяти, присутствовавшего в оригинальном доказательстве (и его упрощении Шенём). Эта техника названа автором «наивной дерандомизацией». Кратко говоря, используя генератор псевдослучайных чисел Нисана–Вигдерсона, эта техника позволяет сильно сократить перебор, если множество, в котором мы ищем, не слишком мало и «просто устроено». Но одной этой техники недостаточно, автор использует еще и так называемый экстрактор Тревисана (точнее его версию, принадлежащую Разу, Рейнгольду и Вадхану).

Использование экстракторов в доказательстве теоремы А. Мучника является само по себе новшеством, принадлежащим диссертанту. Это новшество подробно изучено в третьей главе, где дано новое доказательство теоремы Мучника в исходной формулировке (без ограничений на ресурсы) с помощью экстракторов.

В пятой главе делается попытка перенесения теоремы Мучника на сложность с ограничением времени. При наиболее естественном перенесении результат звучал бы так: программе p достаточно полиномиального времени при условии, что и кратчайшей программе преобразования x в y тоже достаточно полиномиального времени, причём короткая программа преобразования x в p также работает полиномиальное время. В такой, наиболее естественной, формулировке результат не получился, что не удивительно, поскольку его перенесение в этой форме упирается в проблему перебора P=?NP. Полученный автором результат звучит так: существует вероятностная программа p переработки x в y, работающая полиномиальное время при условии сообщения со стороны некоторой информации об y (причём ложная информация может быть программой отбракована, так что при правильных советах программа выдает y, а при неправильных ошибается с очень маленькой вероятностью), и при этом короткая программа преобразования y в p работает полиномиальное время, как и хотелось бы.

Наконец, шестая глава посвящена колмогоровским экстракторам. Это понятие было определено Хичкоком, Паваном и Винодчадраном, которые доказали их существование. Существуют ли колмогоровские экстракторы с ограничением памяти или времени, было неизвестно. Шестая глава восполняет этот пробел для ограничений памяти — в ней доказано существование вычислимой на полиномиальной памяти функции от двух слов со

значением в множестве слов, и имеющей следующее свойство. Если оба входа x, y имеют высокую колмогоровскую сложность с полиномиальным ограничением памяти (скажем, не меньше k), и при этом независимы (сложность пары (x, y) с полиномиальным ограничением памяти примерно равна сумме сложностей x, y), то значение функции является случайным словом длины примерно $2k$ (то есть, его сложность с полиномиальным ограничением памяти также примерно равна длине $2k$). Этот результат также получен техникой «наивной дерандомизации».

Таким образом, в диссертации получены три новых и интересных результата о колмогоровской сложности с ограничением ресурсов. Все результаты диссертации рассказывались на семинарах и конференциях и опубликованы в журнальных статьях автора.

Диссертация удовлетворяет 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.

Научный руководитель
д. ф.-м. н., профессор Н.К. Верещагин

9 сентября 2014 г.

Подпись научного руководителя удостоверяю.
И.о. декана механико-математического факультета
ФГБОУ ВПО МГУ им. М.В. Ломоносова,
профессор В.Н. Чубариков