Отзыв официального оппонента д.ф.-м.н., профессора
Верещагина Н.К.
на диссертацию Кнопа Александра Анатольевича «Сложность эвристических вычислений и интерактивных протоколов» на соискание ученой степени кандидата физико-математических наук по специальности 01.01.06 — математическая логика, алгебра и теория чисел.

Диссертация относится к теории сложности вычислений. В ней получены некоторые новые оценки схемной сложности, упрощены доказательства некоторых теорем об иерархии для эвристических сложностных классов, а также получена одна новая теорема этого вида, и доказаны некоторые теоремы о иерархии для порождаемых (моделируемых) распределений.

Научная ценность. Наиболее значимым результатом является первый из упомянутых выше: для всех k в классе AvgMA существует язык, схемная сложность которого больше n^k, где n обозначает длину входа. В некотором смысле, этот результат устанавливает новый рекорд, поскольку раньше было известно существование таких языков в классах S_2P (Джип-И Цай 2001), PromiseMA и MA/1 (Фортнау–Сантанам 2004), по-видимому не сравнимых с классом AvgMA. Основная идея доказательства заимствована у Фортнау и Сантанама, однако одного этого метода недостаточно, и автор соединил эту идею с «трюком Первышева», позволяющим строить эвристические алгоритмы для языков из PromiseBPP (для подходящих распределений на входах).

Вторым по значимости результатом является новое доказательство теоремы об иерархии для класса HeurBPP. Заслугой диссертанта является блестящая идея изолировать «трюк Первышева» в виде почти очевидной леммы (Лемма 3.1 в диссертации) и использовать теорему Ватсона (2004) о иерархии распределений вероятностей на множестве $\{0,1\}$. Последняя утверждает, что для всех k существует l, для которого для любого натурального n можно за время n^l породить (или вычислить, что в данном случае одно и то же) некоторое распределение вероятностей на множестве $\{0,1\}$, которое нельзя приблизить никаким распределением вероятности, породимым за время n^k. Точнее, статистическое расстояние между двумя распределениями близко к $1/2$. Диссертант также нашел более простое доказательство теоремы Ватсона, чем оригинальное. (На самом деле теорема Ватсона относится к произвольному фиксированному множеству исходов вместо множества $\{0,1\}$, упрощение было получено только для случая двух исходов.) К сожалению, это

упрощенное доказательство в диссертации не приведено (но было послано автором оппоненту по его просьбе отдельным письмом). Теорема об иерархии легко следует из Леммы 3.1 и теоремы Ватсона, и получаемое таким образом доказательство теоремы об иерархии (учитывая упрощение доказательства теоремы Ватсона, найденное диссертантом) в самом деле проще оригинального.

В диссертации также упрощается доказательство теоремы об иерархии для класса HeurNP (Первышев, 2007). Упрощение достигается опять использованием теоремы Ватсона для двух исходов. Кроме этого, в упрощенном доказательстве использован технически сложный результат (Теорема 3.9) из работы Голдрайха (2011) о существовании усреднителя с небольшим количеством случайных бит (усреднитель — это полиномиальный вероятностный алгоритм, приближенно вычисляющей среднее значение данной булевой функции от n переменных, данной алгоритму как внешняя процедура).

Еще в диссертации имеется условная теорема о иерархии: если существует односторонняя функция, то для каждого k даже в классе P есть язык, не распознаваемый эвристическими вероятностными алгоритмами за время n^k. Предположение об односторонних функциях используется для построения генератора ПСЧ. В доказательство опять использована теорема Ватсона, а генератор ПСЧ нужен, чтобы трудное распределение на 0,1, существующее по теореме Ватсона, представить как долю слов данной длины в некотором полиномиально разрешимом языке.

Указанные доказательства теорем об иерархии получены примерно одним и тем же приемом (сведением к теореме Ватсона), который я не встречал раньше, и изобретение которого, по всей видимости, принадлежит диссертанту.

Последняя четвертая глава диссертации посвящена теоремам об иерархии для распределений на множестве слов длины n (а не на небольшом множестве, как в теореме Ватсона), порождаемых в ограниченное время. Наиболее технически сложным результатом диссертанта является теорема 4.1, смысл которой в следующем: если t' существенно меньше t, то за данное время t можно породить распределение на словах длины n, далекое от всех распределений, которые можно породить за время t'. К сожалению, автору удалось доказать это утверждение только для t, t' сверхполиномиально растущих с ростом n. Для полиномиальных ограничений времени аналогичное утверждение открыто.

Общим недостатком всех теорем об иерархии, обсуждающих-

ся в диссертации, является то, что сложный язык (или распределение) является сложным лишь для бесконечно многих n, а не для почти всех n, как хотелось бы. Этот недостаток присущ всем теоремам об иерархии, полученным методом отложенной диагонализации.

Изложение. Введение написано замечательно и позволяет получить хорошее представление о том, что будет дальше. Первая глава (Основные понятия) написана хорошо, впрочем, некоторые понятия и обозначения, используемые в основном тексте (например, $\omega(1)$ и HeurNP), так и остались неопределенными. Классы HeurMA и AvgMA определены интуитивно малопонятным образом (хотя приведенное определение и эквивалентно «правильному»).

К сожалению, эта характеристика не относится к остальным трем главам, текст которых изобилует опечатками и языковыми погрешностями и производит впечатление наскоро переведенного на русский язык текста статей, в которых опубликованы результаты. В последнем убеждает использование таких «недопереведенных» на русский язык слов, как «секция» (вместо «глава», «параграф» или «раздел») и «сэмплируемое» (вместо «порождаемое» или «моделируемое» — последний термин был использован в диссертации Ицыксона для того же самого понятия «samplable»). Впрочем, при некотором усилии доказательства и формулировки можно понять, так что этот недостаток не смертелен.

Важной опечаткой, препятствующей пониманию, является путаница между ε и $1-\varepsilon$. А именно, вместо $\mathrm{Heur}_{\varepsilon}$ во многих местах написано $\mathrm{Heur}_{1-\varepsilon}$ (в формулировке и доказательстве Леммы 2.5, во второй строке и первой строке последнего абзаца на с. 29, четвертой строке на с. 32). Так же имеется путаница между между обозначениями Avg и Heur: в «Целях работы» сказано «Доказать нижние оценки на эвристическую схемную сложность эвристической версии класса MA (то есть HeurMA)», в основных результатах сказано, что доказана нижняя оценка для класса HeurMA, а затем в теореме 2.1, которая и является точной формулировкой этого результата, уже использован класс AvgMA вместо HeurMA. Включение HeurMA в AvgMA упомянуто только вскользь в формулировке Леммы 2.6, а это должно быть сказано либо сразу после их определений, либо во Введении, чтобы объяснить, что из Теоремы 2.1 в самом деле следует первый «основной результат». А еще лучше просто исправить путаницу и написать везде AvgMA. Остальные опечатки и недоумения я привожу в Приложении к настоящему отзыву.

В целом небрежность изложения, допущенная в главах 2–4, не умаляет ценности диссертации, которая производит хорошее впечатление. Все результаты диссертации являются новыми и интересными. Доказательства приведены полностью, их достоверность сомнений не вызывает. Основные результаты были опубликованы в 2013–2016 гг. Автореферат правильно и полно отражает содержание диссертации.

Результаты диссертации были представлены в докладах на международных конференциях "Eighth International Conference on Computability, Complexity and Randomness" (Москва, CCR 2013), The 10th International Computer Science Symposium in Russia" (Иркутск, CSR 2015), "The 26th International Symposium on Algorithms and Computation" (Нагоя, ISAAC 2015), "Problems in Theoretical Computer Science" (Москва, 2015), "Special Semester Program on Complexity Theory" (Санкт-Петербург, 2016), "The 27th International Symposium on Algorithms and Computation" (Сидней, ISAAC 2016).

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.

Официальный оппонент
д. ф.-м. н., профессор Н.К. Верещагин

27 февраля 2017 г.

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

Приложение: список мелких замечаний, вопросов и опечаток.

С. 9 девятая строка сверху. Не объяснено обозначение U (равномерное распределение?)

С. 9 десятая строка сверху. Здесь два раза упомянуто $1/n^c$. Константа c одна и та же в обоих обозначениях? Если это так, то стоит это подчеркнуть.

С. 11. Вопрос 4 совершенно непонятен.

С. 12 четвертая строка снизу. Слева от включения стоит класс языков, а справа — класс распределенных задач. Требуется уточнение.

С. 13 первая строка сверху. Какой квантор по k?

С. 14 «и и»

С. 21 вторая строка сверху. Чем больше b, тем определение слабее. Зачем разрешать дробные значения b?

С. 25 вторая строка сверху. Здесь $f_n(S)$ должно рассматриваться, как мультимножество.

С. 28 одиннадцатая строка снизу. Используется лемма 2.7, а не 2.6.

С. 32 восьмая строка снизу. Пропущено слово *Доказательство.*

С. 39 начало доказательства теоремы 3.3. Для какого параметра a надо применить теорему 3.1? Это не очевидно.

С. 45 одиннадцатая строка снизу. Вместо $1/4$ должно быть $\varepsilon/2$.

С. 46 седьмая строка снизу. Почему не положить a равным b?

С. 51 десятая строка снизу. Вместо A_i должно быть $A_i(1^n)$.

С. 52 во многих местах. Используется не определенное ранее обозначение ε.