УТВЕРЖДАЮ
Директор Института проблем
передачи информации РАН
д.ф.м.н. А.Н.Соболевский
« » февраля 2017 года

Отзыв ведущей организации на диссертацию Кнопа Александра Анатольевича «Сложность эвристических вычислений и интерактивных протоколов», представленную на соискание учёной степени кандидата физико-математических наук по специальности 01.01.06 — математическая логика, алгебра и теория чисел

Без преувеличения можно сказать, что главной задачей в теоретической информатике (и одной из главных — в математике вообще) является получение нижних оценок сложности для конкретных задач. С одной стороны, это показало бы, что в некоторых случаях поиски эффективных алгоритмов обречены на неудачу. С другой стороны — и с практической точки зрения это главное — такие нижние оценки могли бы гарантировать устойчивость практически важных криптографических протоколов относительно атак с реалистически ограниченными вычислительными ресурсами. В отсутствие таких оценок не только конкретные протоколы остаются основанными на недоказанных предположениях (многие — на сложности задачи разложения на множители, например), но и вообще сама возможность криптографических протоколов с передачей данных по открытому каналу остаётся под вопросом.

Не удивительно поэтому, что не получение нижних оценок были направлены большие усилия. К сожалению, задача эта оказалась исключительно трудной и пока что выглядит недоступной для современных методов. Имеющиеся продвижения носят весьма ограниченный характер с точки зрения глобальных целей (и рецензируемая диссертация тут не исключение, естественно), но тем не менее составляют большой и интересный (как технически, так и философски) раздел теоретической информатики, который называют теорией сложности вычислений.

Диссертация посвящена двум разделам теории сложности вычислений, теоремам об иерархии в разных ситуациях (главы 3 и 4) и нижним оценкам

схемной сложности для задач тех или иных сложностных классов (глава 2).

Теоремы об иерархии показывают, что для данного ограничения на ресурсы (скажем, времени работы) существуют задачи, которые с такими ограничениями неразрешимы, хотя и разрешимы с несколько бóльшими ограничениями. Обычным примером такого рода задач являются задачи моделирования вычислений с несколько бóльшим ресурсом, и в простых случаях рассуждение использует стандартный приём, называемый «диагонализацией» — для всякого кандидата в более эффективный алгоритм подбирается вход, на котором этот кандидат работает неправильно. Но в более сложных случаях, когда рассматриваются более сложные классы задач, скажем, соответствующие вероятностным алгоритмам, или «недетерминированным алгоритмам», диагонализация не работает (переход к отрицанию выводит из класса недетерминированно распознаваемых множеств, а вероятностные машины задаются не синтаксически, а семантическим условием, и потому их моделирование не обеспечивает разрыва между вероятностью для утвердительных и отрицательных ответов). Тем не менее в некоторых случаях это доказать удаётся, и такого рода результатам посвящены **третья** и **четвёртая** главы диссертации, содержащие результаты работ [23] и [24] соответственно.

Схемную сложность (булеву сложность, сложность схем из функциональных элементов) начал рассматривать ещё Шеннон. Когда появились другие модели вычислений (уже в 1960-е годы), стало понятно, что схемная сложность является их «неуниформным» вариантом: мы рассматриваем какую-то задачу (скажем, свойство двоичных слов) как серию задач (для каждой длины входа — своя задача), и изучаем, как сложность задач серии растёт с ростом длины входа. В некотором смысле это даже больше соответствует практике, так как обычно нас интересуют задачи какого-то определённого размера, и переход к сложности задачи произвольного размера всего лишь «упрощающее приближение сверху». Достоинством схемной сложности является и то, что она определена достаточно инвариантно: размер схемы умножается не более чем на константу при переходе к другим вариантам определения (изменение базиса). Доказав сверхполиномиальные нижние оценки для какой-то задачи из NP, мы бы получили в качестве немедленного следствия, что $\mathrm{P} \neq \mathrm{NP}$. К сожалению, продвижений в этой задаче мало, для явно заданных функций никаких оценок, кроме линейных, не известно. Поэтому естественно пытаться ослаблять требования и рассматривать всё менее и менее «явные» функции.

Во **второй** главе диссертации в качестве такого ослабленного понятия «явной» функции рассматривают задачи из (униформного) класса HeurMA (эвристического варианта класса MA, соответствующего протоколам диалога Мерлина и Артура — в таком порядке; эвристический вариант допускает, что

для малой доли входов ничего не гарантируется, зато для остальных выполнены обычные условия). Основным результатом (соответствующим номеру 1 в списке на с. 12) является тут теорема 2.1 на с. 28. Она показывает, что существуют языки из класса HeurMA (с полиномиальным ограничением на алгоритм проверки для Артура), которые не лежат даже в аналогичном неуниформном классе, если ограничить размер проверочной схемы конкретным полиномом. Доказательство этой теоремы «неконструктивно» в том смысле, что оно разбирает два случая (некоторый язык имеет полиномиальные схемы или нет), при этом какой из этих случаев имеет место (и тем самым что является примером языка с указанным в теореме свойством) остаётся неясным. Используются методы, восходящие к работе Сантанама [9]; главное достижение тут в том, что удаётся обойтись без «подсказки», перейдя к эвристическим классам (и доказывая отсутствие схем также из эвристических классов)

Вторая группа результатов связана с использованием связи между теоремой об иерархии для распределений, доказанной Ватсоном в [18] (ослабление ограничений на вероятностные алгоритмы приводит к увеличению класса их выходных распределений) и теоремами об иерархии для эвристических классов. Это наблюдение позволило упростить доказательства известных результатов (теорема 3.2 на с. 39, соответствующая п. (2) в перечислении результатов на с. 12, и теорема 3.11 на с. 46, соответствующая п. (3) в этом перечислении), а также получить новые результаты (теорема 3.8, с. 42, соответствующая п. (6), а также теорема 3.6 на с. 41, п. (5) касающиеся классов функций и дающие близкую к 1 нижнюю границу вероятности ошибки для эвристических алгоритмов). В главе 3 приводятся также условные результаты об иерархии (как в предположениях о трудности задач из класса NP, точнее, существования односторонних функций, теорема 3.3 на с. 39, соответствующая п. (4) перечисления, так и в предположении их простоты, теорема 3.4 на с. 40).

В главе 4 доказываются результаты, показывающие, что ограничение на сложность алгоритма порождения распределений может изменить принадлежность задачи эвристическому классу. Теорема 4.1 на с. 50, соответствующая (7) в перечислении на с. 13, сравнивает полиномимальное ограничение на время порождения с чуть большим ($n^{\log^{\epsilon}(n)}$); следствие 4.3 на с. 61, соответствующее (8) в перечислении, сравнивает ограничение на время с фиксированной степенью с произвольным полиномиальным ограничением (правда, с худшей оценкой ошибки, чем в теореме 4.1). Доказательства этих результатов используют технику Ватсона, называемую автором «древесной диагонализацией».

Оценивая диссертацию в целом, можно сказать, что в ней автор развил

имеющиеся техники получения результатов о иерархии и получил много интересных новых результатов, а также обнаружил неожиданную связь между известными результатами (о иерархии для распределений и для эвристических классов).

К сожалению, работа написана не очень аккуратно, и содержит недочёты разной степени серьёзности — от неудачных определений и неясных формулировок до опечаток и ошибок с точки зрения русского языка. Вот несколько примеров:

- с. 20: определение класса AvgMA непонятно, можно уменьшить вероятность ошибки и затем добавить в алгоритм начальный этап, в котором выдаётся отказ с вероятностью $1/8$, в результате дополнительное условие по сравнению с эвристическим классом становится тривиальным;
- определение 2.1 на с. 23 ничего не говорит о времени работы алгоритма A;
- на с. 22 говорится о «самопроверяемости» и «проверяемости ответов» — хотя в предыдущем предложении говорится о «самоисправляемом» и «контролируемом», и никаких указаний, что чему соответствует (и почему терминология вдруг изменена) нет.
- обозначения в разных частях диссертации не согласованы: например, при переходе от формулировки (5) на с. 12 к соответствующей теореме 3.6 на с. 41 буква a заменяется на k, буква k заменяется на b, буква δ заменяется на τ, буква ϵ заменяется на δ, буква f заменяется на F; к тому же в теореме 3.6 пропущена звёздочка в $\{0,1\}^*$; формулировка (6) на с. 13 упоминает неиспользуемый параметр a вместо использующегося в дальнейшем k;
- цели (7) и (8) на с. 12 сформулированы крайне невнятно: обильное употребление кавычек не заменяет указания подразумеваемых кванторов (имеются ли в виду некоторые «простые» распределения или все «простые» распределения, если говорится, что язык “решается на «простых» распределениях”);
- в русском языке «секции» обычно называют «разделами», говорить «докажем иерархию на эвристический аналог» (класса NP) тоже не стоило, хотя можно догадаться, что имеется в виду.
- запуск программы проверки орфографии тоже бы не повредил — она не может заметить все ошибки, но «доказаные» на с. 22, вероятно, были бы обнаружены;

- с. 24: «доказательство из [29] можно перенести»: книга [29] — это стандартный учебник, и следовало бы пояснить, какое именно из многочисленных доказательств имеется в виду;
- с. 24: говорится о «первой части доказательства» и «второго случая», и читатель может лишь гадать, имеются ли в виду части доказательства, случаи в каком-то рассуждении и в чём именно они могли бы состоять.

И так далее.

Отмеченные недостатки, тем не менее, не снижают общей высокой оценки работы диссертанта и не ставят под сомнение её научную ценность.

Диссертационная работа А.А. Кнопа относится к активно развивающемуся и весьма интересному направлению исследований и выполнена на высоком научном уровне. В ней получены новые интересные результаты, уже получившие признание специалистов, и приведены их доказательства. Автореферат соответствует содержанию диссертации.

Результаты диссертации опубликованы в рецензируемых научных изданиях (три публикации в трудах известных международных конференций в области компьютерных наук — ISAAC 2015, ISAAC 2016, CSR 2015). В диссертации указан вклад автора в совместных публикациях.

Работа написана на высоком научном уровне и отвечает требованиям Положения о порядке присуждения учёных степеней, а её автор, Александр Анатольевич Кноп, заслуживает присуждения ему учёной степени кандидата физико-математических наук по специальности 01.01.06 (математическая логика, алгебра и теория чисел).

Кандидат физико-математических наук,
старший научный сотрудник
Института проблем передачи информации РАН
Адрес: 127051, г. Москва, Большой Каретный переулок, д.19 стр. 1
Телефон: +7 (495) 650-42-25
Электронная почта: sasha.shen@gmail.com

Александр Шень

26 февраля 2017 года