# Отзыв официального оппонента на диссертацию Опарина Всеволода Владиславовича «Оценки сложности вывода в системах доказательства, основанных на методе резолюций», представленную на соискание учёной степени кандидата физико-математических наук по специальности 01.01.06 — математическая логика, алгебра и теория чисел

Многие комбинаторные утверждения имеют вид утверждений о несовместности некоторой системы локальных условий. Скажем, утверждение «принципа Дирихле» гласит, что $m$ кроликов нельзя разместить в $n < m$ клетках так, чтобы в каждой клетке было не больше одного кролика. Если ввести булевы переменные $p_{ij}$, истинность которых означает размещение $i$-го кролика в $j$-й клетке, то условие о том, что $i$-й кролик куда-то помещён, можно представить дизъюнкцией $p_{i1} \vee \ldots \vee p_{in}$, а условие о том, что в $j$-ю клетку помещено не более одного кролика, можно представить как набор ограничений $\neg p_{uj} \vee \neg p_{vj}$ (по одному для каждой пары различных $u, v$ из $1 \ldots m$). Собрав все эти ограничения, мы получим формулу в конъюнктивной нормальной форме, невыполнимость которой и утверждается «принципом Дирихле». (Она обозначается $\mathrm{PHP}_n^m$ в соответствии с английским названием “PigeonHole Principle”.)

Другой пример подобного рода — рассуждения, связанные с подсчётом чётности. Например, по этим причинам не существует графа, у которого степень одной вершины была бы нечётна, а степень остальных вершин была бы чётна. Можно даже ограничиться частным случаем, когда степень данной вершины равна 1, а степень всех остальных равна 2 (путь выходит из этой вершины и нигде не кончается — такое невозможно). Этому утверждению соответствует формула, в которой для каждой пары вершин $i, j$ есть переменная $p_{ij}$, означающая ребро между ними — утверждения о степени вершин легко представляются в виде набора клауз (дизъюнктов).

Аналогичным образом можно представить и другие комбинаторные утверждения — скажем, лемму Шпернера (о разноцветном треугольнике в триангуляции), дискретные версии топологических результатов (скажем, об отсутствии непрерывного векторного поля на сфере, если заменить такое поле его дискретным приближением в конечном числе точек сферы) и др.

Возникает естественный вопрос о сравнении различных комбинаторных принципов такого рода по «сложности» или «силе». Этот общий вопрос можно конкретизировать разными способами. В терминах теории сложно-

сти можно определять сложностные классы (например, известный класс PPAD) и спрашивать про сводимость и полноту задач в этих классах. Можно рассматривать модель разрешающих деревьев и спрашивать, например, во скольких вершинах триангуляции нужно проверить цвет, чтобы найти разноцветный треугольник из леммы Шпернера (в этом смысле, скажем, лемма Шпернера существенно отличается от своего одномерного варианта, теоремы о промежуточных значениях: в последнем случае достаточно логарифмического числа проверок благодаря двоичному поиску, а в лемме Шпернера так не получается).

Можно (и именно этот вариант рассматривается в работе) оценивать сложность задачи в терминах минимальной длины вывода в той или иной системе доказательств. Например, можно рассматривать исчисление резолюций и ставить вопрос о том, сколько раз нужно применить правило резолюции к данному невыполнимому набору дизъюнктов (невыполнимой формуле в конъюнктивной нормальной форме), чтобы получить противоречие (пустой дизъюнкт). Правило резолюции позволяет из формул $a \vee b$ и $\neg b \vee c$ получить формулу $a \vee c$, и даёт полное исчисление: из всякой невыполнимой формулы (в частности, соответствующей принципу Дирихле или иному комбинаторному принципу) можно получить противоречие, вопрос только в том, сколько шагов понадобится — скажем, будет ли это число полиномиальным или экспоненциальным. (Для принципа Дирихле имеет место второе.)

Это направление исследований достаточно известно; получены нетривиальные (и в некоторых случаях достигающие друг друга) верхние и нижние оценки. Смысл этого двоякий: во-первых, можно сравнивать задачи по сложности, во-вторых, можно сравнивать «мощность» различных систем доказательств. Изначальная мотивация состояла в том, что вопрос о совпадении классов NP и coNP можно переформулировать как вопрос о существовании системы доказательств (тавтологий, являющихся отрицаниями невыполнимых формул) с полиномиальным ограничением на длину доказательства произвольной тавтологии — так что если эти классы различны, то для всех систем доказательств существуют сверхполиномиальные нижние оценки. Соответственно первым шагом к решению этого вопроса можно было считать получение сверхполиномиальных нижних оценок хоть для каких-то систем доказательств. Сейчас видно, что эта идея далека от воплощения — сверхполиномиальные оценки есть пока лишь для конкретных систем, и методы их получения не обобщаются на более сильные (не говоря уже о произвольных полиномиальных системах доказательств, что нужно для $\mathrm{NP} \neq \mathrm{coNP}$). Но уже полученные результаты тем не менее позволяют сравнивать разные задачи по сложности, а также дают экспоненциальные нижние оценки для времени работы практически важных классов алгоритмов (DPLL и др.)

Диссертация содержит несколько полученных её автором сравнительно независимых результатов. Их можно разбить на три большие группы:

- верхние оценки (которые показывают точность ранее полученных нижних оценок), глава 2 [36,37];
- результаты про обобщённые резолюции (для алфавита из более чем двух букв), глава 3 [35];
- результаты про семейства формул со сдвигом (переменные образуют бесконечную в обе стороны цепочку, и все ограничения и их следствия инварианты относительно сдвига вдоль неё), глава 4 [34].

Верхние оценки в работе есть двух типов: $O(2^n)$ (с точностью до многочлена) для отсутствия совершенного паросочетания в графе (теорема 2.2) и доказательств в исчислении резолюций (как выражается автор, «в общей резолюции»), и $2^{O(n)}$ для древовидных докательств в исчислении резолюций с линейными уравнениями по модулю 2 (RES-LIN) для принципа Дирихле и отсутствия совершенного паросочетания. Для паросочетаний они основаны на критерии Татта отсутствия совершенного паросочетания (даваемое им препятствие с помощью разных приёмов преобразуется в доказательство); для принципа Дирихле использование возможностей сложения по модулю 2 используется для более быстрого отыскания «места неисправности»; это улучшение позволяет сделать доказательство отсутствия паросочетаний древовидным.

Результаты про обобщённые резолюции (для задачи CSP в более чем двухбуквенном алфавите, в качестве которого берутся вычеты по некоторому модулю $k$) касаются в первую очередь обобщённых цейтинских формул. Для построения такой формулы каждое ребро графа помечается переменной, причём на одном конце ставится плюс, а на другом минус. Для каждой вершины налагается условие на переменные, соответствующие инцидентным рёбрам: указывается, чему должна быть равна их сумма (со знаками) по модулю $k$. Эти условия несовместны, если требуемые суммы все вместе не равны нулю по рассматриваемому модулю (и это препятствие единственное, если граф связен). В работе объясняется, как применить известные методы Бен-Сассона и Вигдерсона (связь размера с шириной) для получения нижних оценок (см. неравенства 1 и 2 на с. 55). Показано также (теорема 3.2), как можно для случая древесных доказательств улучшить эти оценки, заменив в них основание степени 2 (которое получается из рассуждений по схеме Бен-Сассона и Вигдерсона) на $k$. Кроме того, показано (теорема 3.3), что сложность доказательства связана с наличием подграфа со свойствами расширения.

Глава 4 посвящена менее классической задаче, в которой ограничения на переменные инварианты относительно сдвига. Пусть есть некоторый конечный набор двоичных слов, которые объявлены «запрещёнными». Можно

поставить вопрос, существует ли бесконечная последовательность нулей и единиц, которая не содержит запрещённых подслов (в эргодической теории говорят, что рассматривается subshift of finite type, который может быть пуст или непуст). Если её нет, то можно установить этот факт «синтаксически», проведя вывод в естественной системе. Если допустить «запрещения с пропуском» (в некоторых местах запрещённых подслов может стоять символ «джокера», который может заменяться нулём или единицей в запрещённом вхождении), то их можно естественно интерпретировать как дизъюнкты исчисления резолюций, в которых дополнительно разрешается сдвиг переменных по цепочке (потому что запрещения относятся к любому месту последовательности). Можно рассматривать исчисление резолюций как в обычном виде, так и с дополнительным правилом сдвига. В главе 4 получены результаты в двух направлениях: (1) как переносить нижние оценки в обычном исчисления на случай исчисления со сдвигом (и модифицированной формулы) [теорема 4.1, следствия 4.1–4.3], и (2) как построить формулу, в которой возможность сдвига сильно уменьшает размер минимального доказательства [теорема 4.2].

* * *

Диссертация относится к давно известной (с 1960-х годов) и активно разрабатываемой в последнее время тематике, имеющей как теоретическое, так и практическое (связанное с трудными формулами для различных систем поиска выполняющих наборов) значение; интересные работы в этой области сделаны коллегами диссертанта по ПОМИ РАН. Можно добавить, что не все результаты диссертанта вошли в диссертацию (его недавняя работа — на другую тему — принята на конференцию SODA 2017).

В работе имеются многочисленные недочёты с точки зрения русского языка и стиля, а также опечатки. Нет смысла приводить их полный перечень, поскольку помехи для чтения они не создают, а перечень этот весьма длинный, — но работа для редактора тут была бы (если бы этот текст предполагался к изданию по-русски). Скажем, писать «равносильные предикаты $P$ и $S$ обозначим $P \equiv S$» не стоит (обозначаются не предикаты, а утверждение об их равносильности), вместо «выполняет» в определении 1.2 следовало бы написать «выполняется» (и поставить знаки модуля у $y_{\Pi_2}$), и так далее. Фраза «Паросочетанием в графе $G = \langle V, E\rangle$ называется множество рёбер $M \subseteq E$ таких, что никакая пара рёбер не имеют общей вершины» была бы хорошим примером для лекции по типичным ошибкам в математических текстах (в ней их минимум четыре). Во введении, объясняя основные результаты и цели работы, автор по необходимости использует понятия и термины, вводимые позже, и, пожалуй, несколько злоупотребляет этим правом (и использованием жаргона) — скажем, говоря о цейтинских формулах (ранее

описанных как формулы, связанные с чётностью) для более чем двухбуквенных алфавитов безо всяких пояснений. Если понимать «описание 1» на с. 28 буквально, то алгоритм не имеет возможности вернуть что-либо кроме UNSAT. Кстати, и употребление переменной $x$ в этом алгоритме двусмысленно (это переменная алгоритма или переменная формулы, предложенная эвристикой $A$?). В библиографии тоже есть странности: в работе [37] один из соавторов (Д. Соколов) почему-то заменён сокращённым «et al.», в работе [32] не указано, что речь идёт (судя по всему) о диссертации Митчелла (указано лишь название).

Отмеченные недостатки не ставят под сомнение ценность диссертационной работы, которая 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: три публикации в трудах известных рецензируемых международных конференций в области компьютерных наук (MFCS, SAT, CSR) и одна в рецензируемом научном журнале “Fundamenta Informaticae”. 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, Всеволод Владиславович Опарин, заслуживает присуждения ему учёной степени кандидата физико-математических наук по специальности 01.01.06 (математическая логика, алгебра и теория чисел).

Официальный оппонент
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

7 ноября 2016 года