ОТЗЫВ

официального оппонента д. ф.-м. н. Д. С. Романова
на диссертационную работу Волков Марии Сабины Александровны «Исследование комбинаторных свойств и оценка вычислительной сложности задач рюкзачного типа», представленную на соискание ученой степени кандидата физико-математических наук по специальности 1.2.3. «Теоретическая информатика, кибернетика».

Актуальность темы диссертационного исследования

Самой разрекламированной (и, действительно, ключевой) нерешенной задачей теории алгоритмов на сегодняшний день является вопрос о равенстве сложностных классов P и NP (P vs NP), включённый американским Математическим институтом Клэя в список из семи так называемых «задач тысячелетия». P и NP — это классы массовых распознавательных проблем, разрешимых за полиномиальное от длины входной записи время на соответственно детерминированных и недетерминированных машинах Тьюринга. (Класс NP можно иначе описывать с помощью сертификатов, полиномиально вычисляемых на детерминированных машинах Тьюринга). Всякая такая массовая распознавательная проблема может быть представлена как проблема распознавания принадлежности слова к языку. Очень важным инструментом в задаче P vs NP оказалось наличие полиномиальной сводимости одного языка к другому, состоящее в существовании такого вычисляемого на детерминированной машине Тьюринга (ДМТ) за полиномиальное от длины входного слова время отображения множества всех слов в алфавите первого из этих двух языков во множество слов в алфавите второго из этих двух языков, что образ (относительно данного отображения) слова в первом алфавите является словом второго языка тогда и только тогда, когда само слово в первом алфавите является словом первого языка. Полиномиальная сводимость позволила естественным образом определить класс так называемых NP-полных задач — задач из класса NP, к которым может быть полиномиально сведена любая задача из класса NP. Класс массовых проблем, решаемых на ДМТ за время, не меньшее, чем время решения какой-то NP-полной задачи, можно охарактеризовать как класс условно труднорешаемых задач. Упоминание условности фиксирует здесь отсутствие на текущий момент неполиномиальных нижних оценок сложности решения NP-полных задач на ДМТ (при тотальной неизвестности полиномиальных по сложности алгоритмов решения NP-полных задач на ДМТ). Отметим, что наличие неполиномиальной нижней оценки сложности решения хотя бы одной NP-полной задачи на ДМТ повлекло бы неполиномиальность сложности решения всех NP-полных задач на ДМТ. NP-полнота задачи распознавания выполнимости конъюнктивной нормальной формы была в 1971 году доказана С. Куком и независимо Л. А. Левиным. В 1972 году Р. Карп опубликовал список из двадцати одной NP-полной задачи. Список базовых NP-полных задач постоянно пополняется. Традиционные темы в статьях о сложности решения NP-полных задач таковы: оценки сложности алгоритмов решения, выделение полиномиально разрешимых подклассов (в том числе установление границ между полиномиально разрешимыми и условно труднорешаемыми подклассами), построение более тонкой сложностной классификации, исследование свойств решений задачи.

Задача о рюкзаке в наиболее простой постановке состоит в максимизации суммарной ценности (стоимости) помещаемых в рюкзак предметов при известном ограничении на объем рюкзака. В конце XIX века задача о рюкзаке была уже известна. Распознавательная постановка задачи о 0–1 рюкзаке, при которой каждый предмет встречается в исходном наборе лишь в одной копии, ценность предметов не учитывается, а распознать требуется возможность полного исчерпания объема рюкзака предметами, в упомянутой статье

Р. Карпа шла в списке NP-полных задач под номером 18, что и сфокусировало значительный интерес математиков к этой задаче в рамках проблематики P vs NP. Исследованиями в области задачи о рюкзаке и ее приложений занимались в том числе такие ученые, как Дж. Б. Мэтьюс, Д. Б. Данциг, П. Колесар, О. Ибарра, Ч. Э. Ким, Р. Ч. Меркл, М. Э. Хеллман, А. Шамир, А. К. Ленстра, Х. В. Ленстра, Л. Ловас, Дж. Лагариас, А. Одлыжко, А. Фриз, Э. Бриккел, М. Фюрст, К. Каннан, С. Мартелло, П. Тот, Р. А. Рюппель, М. Костер, А. Жу, Б. ЛаМаккья, К.-П. Шнорр, Ж. Стерн, М. Ойхнер, Ф. Нгуен, М. ван Хоэй, А. Коскинен, В. К. Леонтьев, Э. Н. Гордеев, Р. М. Колпаков, М. А. Посыпкин, Г. Келлерер, У. Пферши, Д. Пизингер, П. Чу, Дж. Бисли, М. Тангавел, П. Варалакшми, С. Абидин, Лю Цзяян, Би Цзинго, Сюй Сунъянь, Р. З. Халаф, Х. Б. Хабиб, Т. А. Джавад.

Именно к актуальной тематике изучения свойств решений задачи о рюкзаке в зависимости от входных данных и относится рассматриваемая диссертационная работа.

Основные результаты диссертации и их научная новизна

Диссертационная работа содержит ряд новых научных положений, относящихся к комбинаторному анализу допустимых решений задачи о рюкзаке.

С применением техники производящих функций выведены формулы, позволяющие вычислять среднее значение целевой функции по всем допустимым решениям в задаче об ограниченном рюкзаке, а также среднее число допустимых решений по всем вариантам задачи об ограниченном рюкзаке фиксированной размерности (с ограничивающей «объемные» коэффициенты величиной, равной объему рюкзака) с двумя копиями каждого предмета в исходном наборе.

Применительно к задаче о рюкзаке введено понятие сюръективной линейной формы. Установлен критерий сюръективности линейной формы для задачи об ограниченном рюкзаке. Получена нижняя оценка плотности сюръективного рюкзачного вектора для 0–1 рюкзака. Доказано, что для каждой размерности лишь одна линейная форма с неубывающими коэффициентами рюкзачного вектора для 0–1 рюкзака является и сюръективной, и инъективной. Приведены оценки числа сюръективных форм для задачи о 0–1 рюкзаке. Показано, что для сюръективных линейных форм все допустимые решения распознавательной задачи о 0–1 рюкзаке могут быть найдены за время, пропорциональное произведению размерности задачи на количество решений. Исследовано поведение сюръективных форм при сильных модульных преобразованиях, сохраняющих конфигурацию множества решений, но могущих приводить к потере сюръективности. Получены новые результаты для линейных форм с разрывами в области значений. Установлены количественные оценки, связывающие расположение разрывов с коэффициентами формы, и доказана возможность построения формы с любым заданным числом разрывов в допустимых границах, представлен алгоритм полиномиальной сложности синтеза таких форм.

Предложена основанная на сюръективных формах модификация криптосистемы Меркла – Хеллмана. Практическая часть работы включает программную реализацию предложенных алгоритмических методов и результаты вычислительных экспериментов. Проведено тестирование, не обнаружившее противоречий с теоретическими построениями.

Все основные результаты диссертации являются новыми.

Содержание работы

Диссертационная работа объемом 106 страниц состоит из введения, трех глав, заключения и списка использованной литературы.

Во введении обоснована актуальность темы, указаны объект и предмет исследования, сформулированы цель и задачи исследования, перечислены методы исследования, определены научная новизна, охарактеризованы обоснованность и

достоверность полученных результатов, подчеркнуты теоретическая и практическая значимость работы, приведены выносимые на защиту положения, перечислены публикации автора по теме диссертации, описана структура диссертации, а также доказано соответствие диссертации паспорту специальности.

Первая глава состоит из трех параграфов и раздела выводов к главе, при этом она содержит различные варианты постановок задачи о рюкзаке и обзор известных результатов и методов исследования, а также намечает генеральную линию авторского исследовательского подхода. Отметим, что оптимизационная задача об ограниченном рюкзаке формулируется как задача максимизации по всем n-мерным целочисленным векторам $(x_1,\dots,x_n)$ при $x_i \in \{0,1,\dots,m\}$ $(i=\overline{1,n})$ «стоимостной» целевой функции $\sum_{i=1}^{n} c_i x_i$ при имеющемся ограничении на «объемную» линейную форму $\sum_{i=1}^{n} a_i x_i \le b$, где величины a_i, c_i, b — целые неотрицательные $(i=\overline{1,n})$, а m — натуральное число. Вектор $(a_1,\dots,a_n)$ называется рюкзачным. Плотностью рюкзачного вектора называется отношение размерности n к двоичному логарифму максимального элемента этого вектора. При $m=1$ возникает задача о 0–1 рюкзаке.

Во второй главе изложены основные теоретические результаты работы.

С применением техники производящих функций получены аналитические выражения для следующих объектов:

- для степенных рядов, коэффициентами в которых при формальной переменной в степени, равной объему рюкзака, служат многомерные обыкновенные производящие функции, перечисляющие все допустимые решения для этого объема рюкзака в задаче об ограниченном рюкзаке в соответствии со всеми «объемными» и в соответствии со всеми «стоимостными» слагаемыми,
- для числа допустимых решений в задаче об ограниченном рюкзаке,
- для среднего значения целевой функции по всем допустимым решениям в задаче об ограниченном рюкзаке,
- для многомерной обыкновенной производящей функции, перечисляющей все допустимые решения во всех вариантах n-мерной задачи об ограниченном рюкзаке в соответствии со всеми возможными значениями их «объемных» ограниченных одной и той же величиной коэффициентов,
- для среднего числа допустимых решений по всем вариантам n-мерной задачи об ограниченном рюкзаке (с ограничивающей «объемные» коэффициенты величиной, равной объему рюкзака b) с двумя копиями каждого предмета в исходном наборе $(m=2)$.

Следует отметить, что перечисленные выше результаты демонстрируют виртуозность автора диссертации по оперированию с производящими функциями и комбинаторными тождествами, а получение этих результатов было сопряжено с преодолением существенных трудностей.

Естественным образом во второй главе вводятся понятия сюръективной и инъективной линейной формы при условии неубывания коэффициентов. Установлен критерий сюръективности линейной формы для задачи об ограниченном рюкзаке. Получена нижняя оценка плотности сюръективного рюкзачного вектора для 0–1 рюкзака. Доказано, что для каждой размерности лишь одна линейная форма с неубывающими коэффициентами рюкзачного вектора для 0–1 рюкзака является и сюръективной, и инъективной. Приведены оценки числа сюръективных форм для задачи о 0–1 рюкзаке. Доказано, что все допустимые решения распознавательной задачи о 0–1 рюкзаке с сюръективной формой можно найти за время $O(ns)$, где n — размерность задачи, а s — число допустимых решений. Введено понятие сильного модульного умножения для целочисленного вектора. Найдено

математическое ожидание k-й в порядке возрастания компоненты вектора, полученного сильным модульным умножением из вектора с возрастающими компонентами. Выведены леммы, содержащие оценки числа отрезков сюръективности для линейной формы в ряде специальных случаев. Получена верхняя оценка числа отрезков сюръективности для линейной формы, условия на коэффициенты которой отличаются знаком неравенства ровно для одной компоненты от условий сюръективности линейной формы. Предложен полиномиальный алгоритм построения линейной формы n переменных с h разрывами ($h \in [0;\ 2^n - 1]$).

В состоящей из трех параграфов третьей главе рассматриваются вопросы приложений построенной в первых двух главах теории и обсуждаются результаты компьютерных экспериментов. Приводится модификация рюкзачной (ранцевой) криптосистемы Меркла – Хеллмана, использующая технику сюръективных линейных форм. Надежды на устойчивость этой модифицированной криптосистемы связаны как с тем, что в ней не эксплуатируются сверхрастущие последовательности, позволившие А. Шамиру вскрыть оригинальную криптосистему Меркла – Хеллмана, так и с такой относительно высокой плотностью сюръективных рюкзачных векторов, которая должна препятствовать эффективному взлому, основанному на методах редукции решеток. Представленные результаты вычислительных экспериментов не опровергают теоретических построений. Экспериментально проверена устойчивость структур предложенной криптосистемы к методам редукции решеток.

В заключении подводятся итоги диссертационного исследования и формулируются основные выводы по работе.

Список литературы содержит 77 ссылок.

Достоверность и обоснованность результатов

Достоверность полученных в диссертации результатов обеспечивается применением строгого математического аппарата и опорой на фундаментальные положения теории сложности вычислений, дискретной математики и комбинаторного анализа. Все приведенные в работе доказательства лемм, утверждений и теорем выполнены на должном уровне математической строгости.

Обоснованность теоретических положений подтверждается их логической выводимостью из известных результатов в области комбинаторики, теории чисел и теории сложности алгоритмов с помощью классических методов этих разделов математики.

Экспериментальная проверка не выявила расхождений с разработанной теорией. Методика проведения вычислительных экспериментов изложена в диссертации с достаточной степенью подробности.

Основные результаты диссертации опубликованы в 9 научных работах, из которых 5 входят в перечень ВАК рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата или доктора наук, а ещё 4 являются публикациями в сборниках трудов конференций. Работа прошла апробацию на международных и межвузовских научных конференциях.

Теоретическая и практическая значимость

Теоретическая значимость диссертационной работы определяется совокупностью полученных в ней новых научных результатов в области анализа комбинаторной структуры решений задачи о рюкзаке. В работе впервые систематически исследован в связи с задачей о рюкзаке класс сюръективных линейных форм, сформулирован критерий сюръективности линейной формы для задачи об ограниченном рюкзаке, предложен эффективный алгоритм перечисления допустимых решений задачи о 0–1 рюкзаке с сюръективной формой.

Полученные аналитические выражения для среднего значения целевой функции в задаче о рюкзаке и для среднего числа допустимых решений по всем вариантам задачи фиксированной размерности об ограниченном рюкзаке (с ограничивающей «объемные» коэффициенты величиной, равной объему рюкзака) с двумя копиями каждого предмета в исходном наборе вносят вклад в развитие перечислительной комбинаторики.

Предложенные в диссертации методы анализа линейных форм с разрывами в области значений и алгоритмы построения форм с заданным числом разрывов расширяют арсенал средств для изучения связи между параметрами задачи и структурой множества ее решений.

Практическая значимость работы заключается в выделении подкласса задач о рюкзаке с эффективно перечисляемыми допустимыми решениями, в разработке полиномиального алгоритма построения примера задачи о рюкзаке с заданным числом отрезков сюръективности, а также в создании использующей сюръективные формы модификации рюкзачной (ранцевой) криптосистемы Меркла – Хеллмана.

Замечания

Замечания, в основном, носят редакционный характер.

1. На странице 4 в строке 1 сверху неясно, имеется ли в виду Леонард Адлеман (Эйдлмен) или Дэниел Эделмен, там же вместо «Д. Лагариаса» желательно было бы написать «Дж. Лагариаса». На странице 105 в строке 4 сверху вместо фамилий второго и третьего соавторов указаны их имена.
2. Оформительским недостатком диссертации является неуказание авторов формулируемых лемм, утверждений, теорем. Предположение, что их автором всегда является автор диссертации, неверно: так, авторами теоремы 2.2 на странице 44 являются В. К. Леонтьев и Э. Н. Гордеев (о чем, впрочем, можно догадаться по предваряющему замечанию к этой теореме, приводимой без доказательства).
3. Обозначение V_b^{dk} на странице 40 в строке 13 сверху следует признать неудачным. Также неудачно вводимое в строке 3 сверху на странице 45 обозначение $R_p(z_1,\dots,z_n)$ ввиду отсутствия в нём b. В диссертации используются разные обозначения для наибольшего общего делителя (см., например, последнюю строку на странице 55 и третью строку на странице 56). Греческая буква μ используется и для обозначения среднего числа (см., напр., строку 9 снизу на стр. 39), и для обозначения числа отрезков сюръективности (см., напр., строку 8 сверху на стр. 62). В строке 6 на странице 85 используется обозначение $A[i]$ в том же значении, что и a_i ранее; вряд ли эта альтернативность обозначений содержательна.
4. На странице 53 в строке 14 сверху слово «приводит» кажется излишне категоричным ввиду наличия упомянутого четырьмя строками выше единственного «исключения» из формулируемого «правила». Аналогичное замечание касается первого предложения второго снизу абзаца на странице 68.
5. На странице 56 в строке 9 сверху слово «нарушает» следует заменить на «может нарушать», а двумя строками ниже слово «становится» следует заменить на «может при использовании известных алгоритмов становиться». На странице 68 в строке 8 сверху вместо слова «решения» должно быть «известных решений». В третьем снизу абзаце на странице 70 в последнем предложении вместо «задача переходит в область экспоненциальной сложности» должно быть «задача переходит в область экспоненциальной сложности при ее решении методами редукции решеток» (об этом, собственно, и идет речь в данном абзаце). Формулировка утверждения 3.1 на странице 73 нуждается в уточнениях: во-первых, в эту формулировку во избежание неверного понимания требуется внести фразу из преамбулы к данному утверждению о том, что речь идет лишь о нижней оценке сложности в среднем разработанного в

главе 2 алгоритма (именно, алгоритма нахождения всех допустимых решений распознавательной задачи о 0–1 рюкзаке с сюръективной формой), а, во-вторых, как следствие, желательно явно указать, что речь идет о нижней оценке сложности в среднем нахождения всех допустимых решений соответствующей задачи.

6. На странице 62 во втором снизу абзаце речь должна идти не об области определения, а об области значений.
7. На страницах 66–67 в доказательстве теоремы 2.7 желательно было бы привести верхнюю оценку сложности обсуждаемого алгоритма.
8. На странице 73 в строке 13 сверху вместо «$N(l)$» должно быть «$N(L)$».
9. В диссертации часто и без дополнительных пояснений в ориентированных на практические приложения разделах используется знак приближенного равенства, что вызывает вопросы. В частности, неоднократно (например, на странице 74 в строке 4 сверху и ниже) упоминается приближенное значение «$d \approx 1{,}033$» эмпирической границы плотности рюкзачного вектора, вблизи которой известные алгоритмы решения задачи о рюкзаке неэффективны при $n = 200$. Неясно, как это приближенное значение (истинное значение величины чуть больше, это $1 + \frac{\log_2(n/2)}{n}$ при $n = 200$, что равно 1,03321928…) сочетается с нестрогим неравенством «$d \geq 1{,}033$» на странице 76 в строке 3 сверху, а также с приближенными равенствами для той же величины «$d \approx 1{,}031$» на странице 90 в строке 5 сверху (видимо, содержащем опечатку) и «$d \approx 1{,}03$» на странице 96 в строке 10 снизу.
10. Неясно, почему модуль на странице 85 в строках 16–15 снизу выбирается из интервала, тогда как на странице 84 в строке 11 сверху в качестве диапазона для модуля указан отрезок с такими же концами.
11. Несколько выбивается из общей стилистики использование экспоненциального компьютерного представления числа на странице 76 в строке 12 снизу.
12. На странице 9 в строке 14 сверху вместо «3» должно быть «4».
13. Из весьма незначительного количества орфографических опечаток следует упомянуть лишь ошибочное написание слова «множества» в строке 5 сверху на странице 76.
14. В работе достаточно много пунктуационных опечаток, в том числе необоснованно созданных абзацных отступов, пропущенных (зачастую — в формулах) пробелов, отсутствующих или неверных знаков препинания после выключных формул. На странице 45 в строках 3 и 8 сверху многоточие в умножении ошибочно выделено запятыми. Архаично смотрятся знаки умножения в виде звездочек.
15. Большинство переносов в формулах соответствуют англоязычному стандарту, хотя есть и русскоязычные переносы (в том числе на странице 47 в строках 3–1 снизу в одной и той же формуле соседствуют оба варианта переноса).
16. Изредка математическое обозначение в тексте не выделено курсивом (напр., стр. 64, строка 4 сверху). Отметим достаточно массовое ошибочное использование курсива при наборе стандартных математических функций, операторов и т. п. (например, max, min, mod, log). Однако, здесь следует исключить повсеместное курсивное со строчной буквы написание *coef* оператора взятия коэффициента члена степенно́го ряда с минус первой степенью переменной, восходящее к традиции, знакомой рецензенту по замечательному задачнику В. К. Леонтьева «Избранные задачи комбинаторного анализа» (М.: Изд-во МГТУ им. Н. Э. Баумана, 2001): рецензент воспринял указанное начертание как дань уважения автором диссертации ушедшему соавтору-классику.

Все эти замечания не снижают положительного впечатления от диссертации.

Заключение

Диссертационная работа М. С. А. Волков содержит решение актуальной задачи исследования комбинаторных свойств задачи о рюкзаке и установления взаимосвязей между входными параметрами и структурой множества допустимых решений, что соответствует паспорту специальности 1.2.3. «Теоретическая информатика, кибернетика» в рамках пункта 3 «Теория сложности алгоритмов и вычислений».

Основные результаты диссертации обладают научной новизной, имеют теоретическое и практическое значение, интересны для специалистов. Они опубликованы в 9 работах, причем 5 из них входят в перечень ВАК рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата или доктора наук. Результаты диссертации докладывались на международных и межвузовских научных конференциях. Автореферат адекватно отражает содержание диссертации.

Представленная диссертация является завершенной научно-квалификационной работой, основные результаты которой следует рассматривать как решение актуальной задачи в области теоретической информатики и кибернетики.

Диссертационная работа удовлетворяет всем требованиям, предъявляемым ВАК к диссертациям на соискание ученой степени кандидата физико-математических наук, а ее автор, Мария Сабина Александровна Волков, заслуживает присуждения ей ученой степени кандидата физико-математических наук по специальности 1.2.3. «Теоретическая информатика, кибернетика».

Официальный оппонент, профессор кафедры математической кибернетики
факультета вычислительной математики и кибернетики
Федерального государственного бюджетного образовательного
учреждения высшего образования «Московский
государственный университет имени М. В. Ломоносова»
доктор физико-математических наук,
доцент Романов Дмитрий Сергеевич

Подпись удостоверяю
Ведущий специалист по кадрам
Т.Г. Коваленко

08 июня 2026 г.

Адрес места работы оппонента: 119991, Россия, г. Москва, Ленинские горы, Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет имени М. В. Ломоносова», д. 1, строение 52, факультет вычислительной математики и кибернетики, кафедра математической кибернетики. Тел.: +7 (495) 939-17-72. Эл. почта: romanov@cs.msu.ru.

Подпись Дмитрия Сергеевича Романова заверяю.

Декан факультета ВМК
МГУ имени М. В. Ломоносова,
академик РАН И. А. Соколов

08 июня 2026 г.