ОТЗЫВ

официального оппонента к.ф.-м.н. Вялого М.Н.
на диссертацию 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 диссертации

Исследование NP-полных задач — одно из важнейших направлений в теоретической информатике. Отсутствие эффективных алгоритмов решения таких задач приводит к целому ряду вопросов: существование приближенных, эвристических алгоритмов, возможность использования конкретной NP-полной задачи в криптографических приложениях и т. п.

Работа Волков М.С.А. принадлежит к этому направлению теории вычислительной сложности. В работе изучаются задачи рюкзачного типа, которые состоят в проверке принадлежности заданного числа множеству значений линейной формы на (0,1)-векторах. Эта задача является NP-полной. Для нее известны эффективные приближенные алгоритмы решения и субэкспоненциальные алгоритмы. Основной мотивацией работы является вопрос о пригодности задач рюкзачного типа для построения криптосистем. В этом случае становится критически важным различение трудных и простых для решения экземпляров задачи при заданных диапазонах параметров задачи. В частности, для построения криптосистем важно иметь алгоритмы преобразования легкорешаемых экземпляров задачи в труднорешаемые. Для построения таких алгоритмов необходим анализ, качественный и количественный, комбинаторной структуры экземпляров задачи и установление связи характеристик экземпляров задачи с ее трудностью.

Классические подходы к анализу сложности задачи о рюкзаке, сформировавшиеся в 70–80-х годах прошлого столетия, во многом опирались на усредненные асимптотические характеристики и оценки наихудшего случая. Указанным выше вопросам о комбинаторной структуре множества решений уделялось недостаточно внимания. При этом отсутствие классификации экземпляров по степени их трудности затрудняет решение целого ряда практических задач — от синтеза вычислительно сложных структур до выбора оптимальной стратегии поиска решений.

В диссертационной работе предпринята попытка восполнить указанный пробел. В центре внимания автора находятся вопросы, связанные с установлением количественных соотношений между параметрами задачи о рюкзаке и комбинаторными характеристиками порождаемого ею множества решений.

Таким образом, тема диссертационного исследования, посвященная анализу комбинаторной структуры задачи о рюкзаке и разработке на этой основе методов классификации экземпляров с прогнозируемой вычислительной сложностью, представляется актуальной как для развития теории сложности, так и с точки зрения возможных приложений в смежных областях.

Основные результаты и их научная новизна

В диссертационной работе в рамках комбинаторного подхода к анализу задачи о рюкзаке получен ряд новых научных результатов, касающихся структуры множества допустимых решений, а также разработаны методы построения и классификации экземпляров с прогнозируемой вычислительной сложностью.

Одной из центральных тем в работе является анализ сюръективных линейных форм. Под таковыми понимаются формы, для которых множество достижимых на булевом кубе значений образует непрерывный целочисленный интервал. В работе получены

необходимые и достаточные условия сюръективности формы. Установлено, что этим условиям удовлетворяет обширное множество последовательностей коэффициентов, мощность которого растет экспоненциально с ростом размерности задачи. Показано, что сюръективные формы допускают нахождение всех решений за время, линейное по числу переменных и количеству самих решений, что выгодно отличает их от общего случая.

Важным с точки зрения приложений результатом является исследование поведения сюръективных форм при модульных преобразованиях. Обнаружено, что подобные преобразования, сохраняя конфигурацию множества решений, нарушают свойство сюръективности и переводят экземпляр в разряд труднорешаемых для большинства известных алгоритмов. Данный результат предоставляет механизм контролируемого перехода от легкорешаемых случаев к труднорешаемым без изменения структуры решений, что представляет интерес для задач синтеза вычислительно сложных структур.

Другим направлением исследования стало изучение линейных форм с разрывами в области значений. В работе получены оценки числа разрывов и доказана возможность построения линейной формы с любым наперед заданным числом разрывов в границах от нуля до теоретически возможного максимума. Найден полиномиальный алгоритм синтеза таких форм. Предложен способ преобразования форм с разрывами к сюръективным с помощью добавления специально подобранных компонент, что расширяет класс практически решаемых задач.

Результатом в области перечислительной комбинаторики применительно к задаче о рюкзаке является получение аналитических формул для среднего числа допустимых решений и среднего значения целевой функции. С использованием аппарата производящих функций выведены выражения, связывающие эти величины с параметрами задачи для случаев бинарных и ограниченных целочисленных переменных. Полученные формулы могут служить основой для построения оценок в декомпозиционных методах.

В работе также предложен и программно реализован комплекс алгоритмических средств, позволяющий генерировать экземпляры задачи о рюкзаке с заданными свойствами и проводить сравнительный анализ вычислительной сложности. Проведенные вычислительные эксперименты подтвердили корректность теоретических построений и продемонстрировали работоспособность разработанных методов.

Указанные выше результаты являются новыми и дают значительный вклад в теорию решения задач рюкзачного типа. Это обуславливает научную новизну диссертационной работы.

Содержание работы

Диссертация состоит из введения, трех глав, заключения и списка использованной литературы.

Во введении обосновывается актуальность темы диссертации, формулируются цели исследования, описаны научная новизна, теоретическая и практическая значимость работы, а также раскрыты основные положения, выносимые на защиту.

В первой главе дается общая характеристика задач рюкзачного типа, обсуждается их роль в теоретической информатике. Здесь же описаны основные инструменты анализа таких задач. Кроме того, в первой главе формулируются основные задачи исследования: анализ комбинаторных и сложностных свойств экземпляров задач рюкзачного типа.

Вторая глава посвящена анализу комбинаторной структуры линейных форм и оценкам их характеристик. Основным техническим инструментом является метод производящих функций. С его помощью получено соотношение между математическим ожиданием функционала задачи и количеством решений подзадач меньшей размерности. Здесь же получены оценки среднего количества допустимых решений для всех экземпляров заданной размерности, что оказывается важным в построении алгоритмов решения задач рюкзачного типа и классификации экземпляров таких задач по степени их

трудности. Также во второй главе вводятся сюръективные линейные формы и изучаются их свойства. Рассмотрены модульные преобразования сюръективных форм, при которых сохраняется комбинаторная структура решений, но теряется упорядоченность и сюръективность. Такие преобразования важны в криптографических приложениях. В завершение изучен вопрос о формах с разрывами и построен полиномиальный алгоритм построения линейной формы с заданным числом разрывов.

В третьей главе рассматриваются вопросы практического применения полученных результатов. Разработаны методы выбора параметров задач рюкзачного типа, позволяющие конструировать экземпляры с заданной вычислительной сложностью. Проведен анализ влияния размерности, плотности и других параметров на устойчивость задач к известным алгоритмам решения. Внимание уделено использованию модульных преобразований для перехода от легкорешаемых экземпляров к труднорешаемым при сохранении структуры множества решений. Демонстрируется применение предложенных конструкций в модифицированной криптосистеме на основе рюкзачных структур. Представлены результаты вычислительных экспериментов, подтверждающих корректность предложенных методов, а также демонстрирующих их устойчивость к решению при помощи методов редукции базиса решетки.

В заключении подводятся итоги проведенного исследования.

Достоверность и обоснованность результатов

Достоверность результатов диссертации подтверждена строгими математическими доказательствами всех сформулированных теорем и утверждений. Разработанные алгоритмические методы прошли экспериментальную проверку на значительном объеме тестовых данных. Методика проведения вычислительных экспериментов изложена подробно, что обеспечивает возможность их воспроизведения. Основные положения, выносимые на защиту, опубликованы в рецензируемых научных изданиях, в том числе в журналах, рекомендованных ВАК и индексируемых в международных базах цитирования. Основные результаты диссертации докладывались на научных конференциях.

Замечания

Работа выполнена и оформлена на высоком уровне. Тем не менее представляется уместным сделать несколько замечаний.

1. В тексте диссертации используются несколько обозначений для математического ожидания. Это затрудняет чтение и может привести к терминологической путанице.
2. В обзоре результатов о задачах рюкзачного типа (раздел 1.1 диссертации) не упомянуты субэкспоненциальные алгоритмы для задачи о рюкзаке. Такое упоминание представляется желательным с учетом криптографических приложений. Отмечу, что в целом сообщество исследователей задач рюкзачного типа обращает мало внимания на существование субэкспоненциальных алгоритмов для задачи о рюкзаке. Так что это упущение не слишком удивительно.
3. В исследовании свойств форм, получаемых сильным модульным умножением, желательно было бы сформулировать точную задачу об анализе распределения получаемых форм, а не только ограничиться изучением этого распределения в эвристически оправданных упрощающих предположениях. С точки зрения основного направления работы такое ограничение вполне оправдано, однако сама по себе задача оценки получающегося распределения очень интересна и результаты в этом направлении, несомненно, украсили бы работу.
4. Приведенное в работе доказательство леммы 2.6 корректно, но весьма громоздко. Представляется, что его можно было бы упростить введением дополнительных операций с множествами целых чисел, представляемых объединениями отрезков.

5. При изложении метода дополнения линейных форм с целью устранения разрывов в работе не приводится анализ того, как данная процедура влияет на рост числа решений и, как следствие, на итоговую вычислительную сложность задачи.
6. В работе практически не рассматривается вопрос устойчивости полученных характеристик (например, числа решений) к малым возмущениям коэффициентов, что представляет интерес с точки зрения теории возмущений дискретных структур.

Отмеченные замечания не снижают общей высокой оценки диссертационной работы и не ставят под сомнение достоверность и значимость полученных результатов.

Заключение

Диссертационная работа Волков М. С. А. содержит решение актуальной научной задачи, связанной с исследованием комбинаторных свойств задачи о рюкзаке, что соответствует паспорту научной специальности 1.2.3. Основные результаты диссертации обладают научной новизной, имеют теоретическое и практическое значение.

Результаты диссертации опубликованы в 9 работах, из них 5 статей в научных журналах, включенных в перечень рекомендованных ВАК РФ, и 3 работы в трудах международных конференций. Автореферат в полной мере отражает содержание диссертационной работы.

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

Диссертационная работа «Исследование комбинаторных свойств и оценка вычислительной сложности задач рюкзачного типа» удовлетворяет всем требованиям, предъявляемым ВАК к диссертациям на соискание ученой степени кандидата физико-математических наук, а ее автор, Волков Мария Сабина Александровна, заслуживает присуждения ей ученой степени кандидата физико-математических наук по специальности 1.2.3. «Теоретическая информатика, кибернетика».

Официальный оппонент,
старший научный сотрудник
отдела №12 ФИЦ ИУ РАН,
кандидат физико-математических наук
Вялый Михаил Николаевич
119333, Москва, ул. Вавилова, 42
тел. 8-977-285-78-34
эл. почта vyalyi@gmail.com}

_____ (М.Н.Вялый)

«18» мая 2026 г.

Подпись М.Н.Вялого
ЗАВЕРЯЮ
Ученый секретарь ФИЦ ИУ РАН
д.т.н. В.Н.Захаров

_____ (В.Н.Захаров)