

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

УДК 519.16

DOI 10.17223/20710410/63/8

КОМБИНАТОРНЫЕ СВОЙСТВА ЗАДАЧИ ОБ ОГРАНИЧЕННОМ РЮКЗАКЕ

М. С. А. Волков

*Московский государственный технический университет им. Н. Э. Баумана, г. Москва,
Россия*

E-mail: sabina-volkoff@yandex.ru

Рассматриваются комбинаторные свойства множества решений в задаче об ограниченном рюкзаке. Как и в общем случае, эта задача является NP-полной задачей комбинаторной оптимизации и её точное решение требует применения алгоритмов перебора с декомпозицией множества допустимых решений. В связи с этим актуален вопрос определения и оценки свойств множества допустимых решений. Получены формулы, позволяющие вычислять среднее значение функционала задачи на множестве её допустимых решений и мощность этого множества через число решений подзадач меньшей размерности. Базовой техникой получения результатов служит метод производящих функций. Рассмотрена задача о рюкзаке с произвольными значениями переменных, в которой совпадают коэффициенты вектора ограничений и целевой функции. Для неё предполагается «сюръективность» множества решений. Найдены оценки значений функционала в этой задаче. Результаты могут представлять интерес для конструирования вычислительных алгоритмов нахождения и оценки числа решений и значения функционала на оптимальных решениях. Найденные выражения также могут быть использованы во вспомогательных процедурах для оценки оптимальности решения в декомпозиционных или эвристических алгоритмах решения задачи о рюкзаке.

Ключевые слова: задача о рюкзаке, производящие функции, NP-полные задачи, метод коэффициентов, вычет, методы декомпозиции.

COMBINATORIAL PROPERTIES OF THE BOUNDED KNAPSACK PROBLEM

M. S. A. Volkov

Bauman Moscow State Technical University, Moscow, Russia

The combinatorial properties of the set of solutions to the bounded knapsack problem are considered. As in the general case, this problem is an NP-complete combinatorial optimization problem and its exact solution requires the use of search algorithms with the decomposition of a set of feasible solutions. In this regard, the question of determining and evaluating the properties of the set of acceptable solutions to the problem is relevant. In this paper, formulas are obtained which allow to calculate the

average value of the functional of a problem on the set of its feasible solutions and the power of this set through the number of solutions of subtasks of smaller dimension. The basic technique for obtaining results is the method of generating functions. We also consider the knapsack problem with arbitrary values of variables, in which the coefficients of the constraint vector and the objective function coincide. For this, the “continuity” of the set of solutions is assumed. Estimates of the values of the functional in this problem are found. The results may be of interest for the design of computational algorithms for finding and estimating the number of solutions and the value of the functional for optimal solutions. The expressions found can also be used in auxiliary procedures to evaluate the optimality of the solution in decomposition or heuristic algorithms for solving the knapsack problem.

Keywords: *knapsack problem, generating functions, NP-complete problems, coefficient method, deduction, decomposition methods.*

Введение

Задача об ограниченном рюкзаке — это вариант классической задачи о рюкзаке, в которой каждый предмет доступен в определённом ограниченном количестве. Имеется набор предметов, содержащий m копий каждого предмета, где k -й предмет ($1 \leq k \leq n$) имеет два неотрицательных целочисленных параметра — вес a_k и ценность c_k . Определено ограничение грузоподъёмности рюкзака b . Задача состоит в том, чтобы выбрать подмножество предметов с максимальной общей ценностью, суммарный вес которого не превышает грузоподъёмности рюкзака. В виде оптимизации задача об ограниченном рюкзаке задаётся выражением [1]

$$\sum_{j=1}^n c_j x_j \rightarrow \max; \quad (1)$$

$$\sum_{i=1}^n a_i x_i \leq b, \quad (2)$$

где $x = (x_1, \dots, x_n)$ — n -мерный вектор с целочисленными компонентами $x_i \in \{0, 1, \dots, m\}$; c_1, \dots, c_n , a_1, \dots, a_n , b — неотрицательные целые числа.

Так как задача (1), (2) является NP-полной и для получения её точного решения используются переборные и декомпозиционные алгоритмы, то актуален вопрос о связи сложности задачи со сложностью её подзадач меньшей размерности. В эвристических подходах используются процедуры получения приближённых оценок значений функционала и распределения значений функционала в области допустимых значений переменных, поэтому формулы для вычисления таких оценок могут непосредственно применяться в подобных алгоритмах либо служить для сравнения используемых алгоритмов.

Для доказательства основных результатов в данной работе использован метод производящих функций. Базовой техникой для выражения ограничений на множество допустимых решений послужил метод коэффициентов. Данный метод определяет линейный функционал на множестве формальных степенных рядов с конечным числом членов отрицательной степени, который ставит в соответствие каждому степенному ряду коэффициент при его члене в минус первой степени. Для степенных рядов, сходящихся в окрестности нуля, этот коэффициент совпадает с вычетом в точке ноль. В ряде случаев этот метод существенно удобнее классического варианта с применением вычетов. Подробное описание метода приведено в [2].

Задача о рюкзаке и её разновидности находят применение в области математического программирования, в частности в теории кодирования и криптографии [3, 4]. Например, задача о рюкзаке стала основой для нескольких криптографических систем, безопасность которых зависит от сложности получения её решения [5]. Поскольку различные вариации задачи о рюкзаке часто возникают при ослаблении задач целочисленного программирования, она интенсивно изучалась в последние десятилетия. Как следствие, литература по ней обширна и охватывает как вопросы, связанные с разработкой алгоритмов, так и теоретические аспекты, связанные со свойствами задачи. Алгоритмическая сторона рассматривается, например, в работах [1, 6].

В последнее десятилетие широкое распространение получило применение эвристических и метаэвристических подходов к решению данной задачи. В [7] предложен алгоритм амебоидного организма для решения задачи о 0-1 рюкзаке. В работе [8] авторы использовали алгоритм когортного интеллекта — метод оптимизации, навеянный естественной склонностью людей учиться друг у друга. Модифицированный генетический алгоритм для решения задачи о многомерном рюкзаке, основанный на предварительном анализе данных, предложен в [9]. В [10] для решения многомерной задачи о рюкзаке представлена эвристика, основанная на методе поиска гармонии. В этом алгоритме внимание уделяется распределению вероятностей значений переменных вместо поиска их точного значения. Гибридный алгоритм решения задачи о 0-1 рюкзаке, основанный на разделении предметов по регионам по степени «жадности», построен в работе [11]. В [12] разработана эвристика, сочетающая методы уменьшения размерности задачи, основанные на правилах фиксации переменных, с решением результирующей целочисленной линейной задачи. В [13] авторы представили переформулировку многомерной задачи о рюкзаке с множественным выбором как задачи разделения множества, позволяющую уменьшить размерность задачи при сохранении общего числа переменных и ограничений.

Распространение получили также работы, связанные с исследованием свойств области допустимых решений в задачах о рюкзаке. В [14] реализован распределённый итерационный метод с фиксированной точкой для решения задачи выполнимости рюкзачных ограничений. В работе [15] предложены полиномиальные по времени алгоритмы оценки числа решений отдельных ограничений. В [16] изучается структура многогранников задач о рюкзаке специального вида. Исчерпывающий обзор последних исследований рюкзачных многогранников приведён в [17].

В данной работе получены комбинаторные формулы, позволяющие вычислять и оценивать значения функционала в зависимости от набора заданных параметров задачи. В п. 1 приведены вспомогательные утверждения, выражающие производящие функции в виде полиномов для множества допустимых решений и значений функционала задачи на этом множестве. В п. 2 найдены выражения для числа решений и математического ожидания значения функционала задачи через число решений подзадач меньшей размерности. В п. 3 рассмотрен случай совпадения коэффициентов вектора ограничений и целевой функции, найдены оценки функционала при его сюръективности на всём множестве решений. Ряд результатов с применением подхода на основе метода производящих функций для задачи о рюкзаке с булевыми переменными приведён в работах [18, 19]. Этот подход использован и в настоящей работе для получения формул для случая ограниченного рюкзака с возможностью повторения предметов.

1. Вспомогательные утверждения

Выразим производящие функции в виде полиномов для множества допустимых решений и значений функционала задачи на этом множестве. Множество допустимых решений задачи V_b — это множество n -мерных векторов x , $x_i \in \{0, 1, \dots, m\}$, $i = 1, \dots, n$, удовлетворяющих неравенству (2). По аналогии с непрерывным случаем будем называть множество V_b многогранником допустимых решений задачи. Объёмом V_b назовём число $|V_b|$ допустимых решений неравенства (2).

Для анализа распределения точек в многограннике V_b используется полином

$$P_b(z_1, z_2, \dots, z_n) = \sum_{x \in V_b} z_1^{a_1 x_1} z_2^{a_2 x_2} \dots z_n^{a_n x_n}. \quad (3)$$

Для исследования свойств значений функционала задачи (1), (2) в допустимых точках многогранника решений будем рассматривать полином

$$F_b(z_1, z_2, \dots, z_n) = \sum_{x \in V_b} z_1^{c_1 x_1} z_2^{c_2 x_2} \dots z_n^{c_n x_n}. \quad (4)$$

Примеры использования этих полиномов для получения оценок в различных типах задачи о рюкзаке приведены в работах [20, 21].

Лемма 1. Для задачи об ограниченном рюкзаке (1), (2) справедлива формула

$$\sum_{b=0}^{\infty} P_b(z_1, \dots, z_n) u^b = \frac{(1 + (z_1 u)^{a_1} + \dots + (z_1 u)^{m a_1}) \dots (1 + (z_n u)^{a_n} + \dots + (z_n u)^{m a_n})}{1 - u}. \quad (5)$$

Доказательство. Преобразуем сумму (3), используя метод коэффициентов. Внутреннее суммирование проводится по всему множеству векторов (x_1, x_2, \dots, x_n) с координатами из $\{0, 1, \dots, m\}$. Использование метода коэффициентов позволяет отбирать из этого множества только векторы, удовлетворяющие ограничениям (2):

$$\begin{aligned} P_b(z_1, \dots, z_n) &= \sum_{t=0}^b \sum_{\{x_1, \dots, x_n\}} z_1^{a_1 x_1} z_2^{a_2 x_2} \dots z_n^{a_n x_n} \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{\sum_{i=1}^n a_i x_i}{u^{t+1}} du = \\ &= \frac{1}{2\pi i} \oint_{|u|=\rho} \sum_{t=0}^b \frac{1}{u^{t+1}} \sum_{x_1=0}^m (z_1 u)^{a_1 x_1} \dots \sum_{x_n=0}^m (z_n u)^{a_n x_n} du = \\ &= \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{u^{-(b+2)} - u^{-1}}{u^{-1} - 1} \prod_{k=1}^n (1 + (z_k u)^{a_k} + \dots + (z_k u)^{m a_k}) du. \end{aligned}$$

Раскладывая полученное выражение по числителю дроби, имеем

$$\begin{aligned} P_b(z_1, \dots, z_n) &= \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{1}{u^{b+1}(1-u)} \prod_{k=1}^n (1 + (z_k u)^{a_k} + \dots + (z_k u)^{m a_k}) du + \\ &\quad + \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{1}{(1-u)} \prod_{k=1}^n (1 + (z_k u)^{a_k} + \dots + (z_k u)^{m a_k}) du. \end{aligned}$$

Ввиду теоремы о вычетах, последнее слагаемое равно нулю; окончательно получим

$$P_b(z_1, \dots, z_n) = \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{1}{u^{b+1}(1-u)} \prod_{k=1}^n (1 + (z_k u)^{a_k} + \dots + (z_k u)^{m a_k}) du. \quad (6)$$

Воспользуемся правилом снятия коэффициента [2]:

$$\frac{1}{2\pi i} \oint_{|u|=\rho} A(u) du = \underset{u}{\text{coef}}\{A(u)\} = a_{-1},$$

где a_{-1} — коэффициент при минус первой степени многочлена $A(u)$.

Подставляя выражение (6) в левую часть формулы (5), получим

$$\begin{aligned} \sum_{b=0}^{\infty} P_b(z_1, \dots, z_n) u^b &= \sum_{b=0}^{\infty} u^b \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{1}{u^{b+1}(1-u)} \prod_{k=1}^n (1 + (z_k u)^{a_k} + \dots + (z_k u)^{m a_k}) du = \\ &= \sum_{b=0}^{\infty} u^b \underset{u}{\text{coef}} \left\{ \frac{1}{u^{b+1}(1-u)} \prod_{k=1}^n (1 + (z_k u)^{a_k} + \dots + (z_k u)^{m a_k}) \right\}. \end{aligned}$$

Теперь, воспользовавшись правилом замены переменной [2]

$$\sum_{k=0}^{\infty} z^k \underset{u}{\text{coef}}\{A(u)u^{-k-1}\} = A(z)$$

для u , получим искомое соотношение. ■

Следствие 1. Для объёма области допустимых решений задачи (1), (2) с $m \in \mathbb{N}$ имеет место равенство

$$|V_b| = \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{(1 + u^{a_1} + \dots + u^{m a_1}) \dots (1 + u^{a_n} + \dots + u^{m a_n})}{(1-u)u^{b+1}} du. \quad (7)$$

Здесь и далее параметр ρ удовлетворяет условиям $0 < \rho < 1$.

Доказательство. Для нахождения числа допустимых решений задачи необходимо подставить $z = 1$ в ряд (3) и провести рассуждения, аналогичные доказательству леммы 1. ■

Лемма 2. Имеет место равенство:

$$F_b(z_1, \dots, z_n) = \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{(1+z_1^{c_1}u^{a_1}+\dots+z_1^{m c_1}u^{m a_1}) \dots (1+z_n^{c_n}u^{a_n}+\dots+z_n^{m c_n}u^{m a_n})}{(1-u)u^{b+1}} du. \quad (8)$$

Доказательство. Преобразуем сумму (4), используя метод коэффициентов. Аналогично лемме 1, введение интеграла позволяет получить ограничение области допустимых решений задачи:

$$\begin{aligned} F_b(z_1, \dots, z_n) &= \sum_{t=0}^b \sum_{\{x_1, \dots, x_n\}} z_1^{c_1 x_1} z_2^{c_2 x_2} \dots z_n^{c_n x_n} \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{u^{\sum_{i=1}^n a_i x_i}}{u^{t+1}} du = \\ &= \frac{1}{2\pi i} \oint_{|u|=\rho} \sum_{t=0}^b \frac{1}{u^{t+1}} \sum_{x_1=0}^m (z_1^{c_1} u^{a_1})^{x_1} \dots \sum_{x_n=0}^m (z_n^{c_n} u^{a_n})^{x_n} du = \\ &= \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{1}{u^{b+1}(1-u)} \prod_{k=1}^n (1 + z_k^{c_k} u^{a_k} + \dots + z_k^{m c_k} u^{m a_k}) du. \end{aligned} \quad (9)$$

Напомним, что метод коэффициентов — это выражение коэффициента при минус первой степени переменной через сумму вычетов, что имеет тот же смысл, что и интеграл Коши в формуле (8). Таким образом, выражение (9) эквивалентно интегралу (8). ■

2. Свойства функционала в задаче об ограниченном рюкзаке

Для эффективного решения задачи о рюкзаке при помощи алгоритмов декомпозиции и перебора необходимо иметь способы оценки значений функционала решений задачи. В этом контексте может быть полезна формула, которая выражает среднее значение функционала на множестве допустимых решений.

Рассмотрим производящую функцию (3), которая характеризует распределение значений функционала $f(x_1, \dots, x_n) = \sum_{j=1}^n c_j x_j$ задачи (1), (2). Для целого неотрицательного k обозначим через A_k число допустимых решений задачи, для которых $f(x_1, \dots, x_n) = k$. Также введём следующее обозначение:

$$\Phi_b(z) = F_b(z, \dots, z) = \sum_{x \in V_b} z^{c_1 x_1} z^{c_2 x_2} \dots z^{c_n x_n} = \sum_{k=0}^{\infty} A_k z^k. \quad (10)$$

Из введённых определений, обозначений и формулы (10) следует соотношение

$$|V_b| = \Phi_b(1) = F_b(1, \dots, 1) = \sum_{x \in V_b} 1^{c_1 x_1} 1^{c_2 x_2} \dots 1^{c_n x_n} = \sum_{k=0}^{\infty} A_k.$$

В частности, заметим, что

$$\max_{x \in V_b} f(x_1, \dots, x_n) = \max_{x \in V_b} \sum_{j=1}^n c_j x_j = \max_{k: A_k \geq 1} k.$$

Далее из леммы 2 получим формулу

$$\Phi_b(z) = \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{(1 + u^{a_1} z^{c_1} + \dots + u^{m a_1} z^{m c_1}) \dots (1 + u^{a_n} z^{c_n} + \dots + u^{m a_n} z^{m c_n})}{(1 - u) u^{b+1}} du. \quad (11)$$

Будем считать, что все точки многогранника V_b равновероятны. Тогда значения функционала $f(x_1, \dots, x_n)$ — это случайная величина $\xi = \xi(a_1, \dots, a_n, c_1, \dots, c_n, b)$ с производящей функцией вероятностей $P(z) = \frac{\Phi_b(z)}{\Phi_b(1)}$. Обозначим её математическое ожидание $\mu(\xi)$. Математическое ожидание (первый момент) случайной величины определяется первой производной её производящей функции вероятностей в точке $z = 1$.

Для определения первой производной функции $P(z)$ введём обозначение

$$\phi(z, u) = \prod_{k=1}^n (1 + z^{c_k} u^{a_k} + \dots + z^{m c_k} u^{m a_k}).$$

Тогда производная функции $\phi(z, u)$ имеет следующий вид:

$$\begin{aligned} & \phi'(z, u) = \\ & = \sum_{k=1}^n \left((c_k z^{c_k-1} u^{a_k} + 2c_k z^{2c_k-1} u^{2a_k} + \dots + m c_k z^{m c_k-1} u^{m a_k}) \prod_{\substack{i=1, \\ i \neq k}}^n (1 + z^{c_i} u^{a_i} + \dots + z^{m c_i} u^{m a_i}) \right). \end{aligned}$$

Выражая её через $\phi(z, u)$, получим

$$\phi'(z, u) = \sum_{k=1}^n \frac{c_k z^{c_k-1} u^{a_k} + 2c_k z^{2c_k-1} u^{2a_k} + \dots + m c_k z^{m c_k-1} u^{m a_k}}{(1 + z^{c_k} u^{a_k} + \dots + z^{m c_k} u^{m a_k})} \phi(z, u).$$

Отсюда найдём значение первой производной функции $\Phi_b(z)$:

$$\Phi'(z) = \frac{1}{2\pi i} \oint_{|u|=\rho} \sum_{k=1}^n \frac{c_k z^{c_k-1} u^{a_k} + 2c_k z^{2c_k-1} u^{2a_k} + \dots + mc_k z^{mc_k-1} u^{ma_k}}{(1 + z^{c_k} u^{a_k} + \dots + z^{mc_k} u^{ma_k})} \frac{\phi(z, u)}{(1-u)u^{b+1}} du.$$

Подставив в это выражение $z = 1$, получим

$$\Phi'(1) = \frac{1}{2\pi i} \oint_{|u|=\rho} \sum_{k=1}^n \frac{c_k u^{a_k} + 2c_k u^{2a_k} + \dots + mc_k u^{ma_k}}{(1 + u^{a_k} + \dots + u^{ma_k})} \frac{\prod_{i=1}^n (1 + u^{a_i} + \dots + u^{ma_i})}{(1-u)u^{b+1}} du. \quad (12)$$

Для каждой из n переменных введём $m+1$ «сечений» множества допустимых решений задачи V_b следующим образом. Для переменной x_k ($1 \leq k \leq n$) «сечение» с номером d ($0 \leq d \leq m$) содержит все решения, удовлетворяющие условию

$$\sum_{\substack{i=1, \\ i \neq k}}^n a_i x_i \leq b - da_k, \quad x_i \in \{0, 1, \dots, m\}.$$

Эти решения соответствуют подмножеству решений задачи (1), (2) с $x_k = d$. Обозначим это множество через V_b^{dk} . Из следствия 1 получаем

$$|V_b^{dk}| = \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{\prod_{i=1, i \neq k}^n (1 + u^{a_i} + \dots + u^{ma_i})}{(1-u)u^{b+1-dak}} du. \quad (13)$$

Теорема 1. Справедливо соотношение

$$\mu(\xi) = \frac{1}{|V_b|} \sum_{k=1}^n c_k (|V_b^{1k}| + 2|V_b^{2k}| + \dots + m|V_b^{mk}|). \quad (14)$$

Доказательство. Вспомним, что $P(z) = \Phi_b(z)/\Phi_b(1)$ и математическое ожидание случайной величины выражается как первая производная её производящей функции $P(z)$ в точке $z = 1$:

$$\mu(\xi) = P'(1) = \frac{\Phi'_b(1)}{\Phi_b(1)}. \quad (15)$$

По формуле (11) имеем

$$\Phi'(1) = \frac{1}{2\pi i} \oint_{|u|=\rho} \sum_{k=1}^n \frac{c_k u^{a_k} + 2c_k u^{2a_k} + \dots + mc_k u^{ma_k}}{1 + u^{a_k} + \dots + u^{ma_k}} \frac{\prod_{i=1}^n (1 + u^{a_i} + \dots + u^{ma_i})}{(1-u)u^{b+1}} du.$$

Разложим это выражение по первому множителю на m слагаемых:

$$\begin{aligned} \Phi'(1) &= \frac{1}{2\pi i} \oint_{|u|=\rho} \sum_{k=1}^n \left(\frac{c_k u^{a_k}}{(1-u)u^{b+1}} \frac{\prod_{i=1}^n (1 + u^{a_i} + \dots + u^{ma_i})}{1 + u^{a_k} + \dots + u^{ma_k}} + \right. \\ &\quad \left. + \frac{2c_k u^{2a_k}}{(1-u)u^{b+1}} \frac{\prod_{i=1}^n (1 + u^{a_i} + \dots + u^{ma_i})}{1 + u^{a_k} + \dots + u^{ma_k}} + \dots + \frac{mc_k u^{ma_k}}{(1-u)u^{b+1}} \frac{\prod_{i=1}^n (1 + u^{a_i} + \dots + u^{ma_i})}{1 + u^{a_k} + \dots + u^{ma_k}} \right) du. \end{aligned}$$

Теперь вынесем c_k за знак интеграла и заметим, что слагаемые данного выражения содержат правые части выражений (13) для $d = 1, \dots, m$:

$$\begin{aligned} \Phi'(1) &= \sum_{k=1}^n \left(c_k \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{\prod_{i=1, i \neq k}^n (1+u^{a_i} + \dots + u^{ma_i})}{(1-u)u^{b+1-a_k}} du + \right. \\ &\quad \left. + 2c_k \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{\prod_{i=1, i \neq k}^n (1+u^{a_i} + \dots + u^{ma_i})}{(1-u)u^{b+1-2a_k}} du + \dots + mc_k \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{\prod_{i=1, i \neq k}^n (1+u^{a_i} + \dots + u^{ma_i})}{(1-u)u^{b+1-ma_k}} du \right). \end{aligned}$$

С учетом равенств (13) произведём замены интегралов их обозначениями и получим соотношение

$$\Phi'_b(1) = \sum_{k=1}^n c_k (|V_b^{1k}| + 2|V_b^{2k}| + \dots + m|V_b^{mk}|).$$

Из выражений (11) и (7) следует

$$\Phi_b(1) = |V_b| = \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{(1+u^{a_1} + \dots + u^{ma_1}) \dots (1+u^{a_n} + \dots + u^{ma_n})}{(1-u)u^{b+1}} du.$$

Подставляя найденные значения в (15), получим искомое соотношение (14). ■

Выражение (14) может быть полезным при оценке эффективности алгоритмов, применяемых для решения задач о рюкзаке. В частности, среднее значение оптимизируемого функционала задачи может служить показателем качества решения при сравнении с результатами, полученными с применением эвристических или аппроксимационных алгоритмов. Если значения, полученные таким алгоритмом, существенно превышают среднее значение функционала, это говорит о том, что алгоритм обеспечивает решения, близкие к оптимальным. Кроме того, данная формула может быть применена для нахождения нижней оценки оптимального значения функционала задачи на подобласти допустимых значений переменной при использовании алгоритмов декомпозиции, например в методе ветвей и границ.

Выражение $|V_b|$ также можно представить через сумму $|V_b^{dk}|$, раскладывая по скобке, соответствующей переменной x_k :

$$|V_b| = \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{(1+u^{a_1} + \dots + u^{ma_1}) \dots (1+u_n^a + \dots + u^{ma_n})}{(1-u)u^{b+1}} du.$$

Домножим и разделим на $(1+u^{a_k} + \dots + u^{ma_k})$:

$$|V_b| = \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{(1+u^{a_k} + \dots + u^{ma_k})}{(1+u^{a_k} + \dots + u^{ma_k})} \frac{(1+u^{a_1} + \dots + u^{ma_1}) \dots (1+u^{a_n} + \dots + u^{ma_n})}{(1-u)u^{b+1}} du.$$

Разложим теперь по числителю $(1 + u^{a_k} + \dots + u^{m a_k})$ на $(m+1)$ слагаемых и заметим, что они содержат выражения (13) для $d = 0, \dots, m$:

$$\begin{aligned} |V_b| &= \left(\frac{1}{2\pi i} \oint_{|u|=\rho} \frac{\prod_{i=1, i \neq k}^n 1 + u^{a_i} + \dots + u^{m a_i}}{(1-u)u^{b+1}} du + \right. \\ &\quad \left. + \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{\prod_{i=1, i \neq k}^n 1 + u^{a_i} + \dots + u^{m a_i}}{(1-u)u^{b+1-a_k}} du + \dots + \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{\prod_{i=1, i \neq k}^n 1 + u^{a_i} + \dots + u^{m a_i}}{(1-u)u^{b+1-m a_k}} du \right). \end{aligned}$$

Заменяя интегралы их обозначениями из (13), получим

$$|V_b| = |V_b^{0k}| + |V_b^{1k}| + \dots + |V_b^{mk}|. \quad (16)$$

Такой метод вычисления числа решений задачи может быть эффективнее прямого подсчёта, поскольку данная формула декомпозирует решение задачи на подзадачи меньшей размерности. При этом области допустимых значений для этих подзадач вложены друг в друга, т. е. $V_b^{di} \subset V_b^{ci}$ при $d \leq c$ для всех $i = 1, \dots, n$, поэтому при последовательном вычислении $|V_b^{di}|$ для $d = 1, \dots, m$ можно использовать $|V_b^{di}|$ при нахождении $|V_b^{ci}|$, $c = d, \dots, m$, что сокращает объём вычислений.

Формула (16) позволяет также сократить количество рассчитываемых значений в (14). Для этого достаточно подставить в (14) значение $|V_b|$, определённое по формуле (16) для какой-нибудь одной переменной x_j , например наименьшего значения a_j . Тогда

$$\begin{aligned} \mu(\xi) &= \frac{1}{|V_b|} \sum_{k=1}^n c_k (|V_b^{1k}| + 2|V_b^{2k}| + \dots + m|V_b^{mk}|) = \\ &= \frac{1}{|V_b^{0j}| + |V_b^{1j}| + \dots + |V_b^{mj}|} \sum_{k=1}^n c_k (|V_b^{1k}| + 2|V_b^{2k}| + \dots + m|V_b^{mk}|). \end{aligned}$$

Вычисление среднего значения функционала по данной формуле также удобно, поскольку оно может выполняться параллельно. Ввиду того, что «сечения» V_b^{di} по каждой переменной i представляют собой непересекающиеся подмножества, значения их объёмов $|V_b^{di}|$ могут быть вычислены независимо, а затем просуммированы для получения среднего значения. Такой подход может значительно ускорить процесс вычислений, особенно при работе с большими экземплярами задач.

Формулы (14) и (16) могут быть уточнены для учёта уникальных особенностей начальных условий при изучении задач, возникающих в конкретных областях применения. Например, в криптографии интерес представляет решение задачи о рюкзаке в несколько изменённом виде: известно, что уравнение $\sum_{i=1}^n a_i x_i = b$ имеет решение в числах $\{0, 1\}$, и требуется найти это решение. В этом случае выражение (14) имеет вид

$$\mu(\xi) = \frac{1}{|V_b|} \sum_{k=1}^n a_k |V_b^{1k}|.$$

Данная формула выражает среднее значение допустимых решений задачи $\sum_{i=1}^n a_i x_i \leq b$ и может применяться для определения вероятности успешной атаки на рюкзачные криптосистемы методом перебора.

Проиллюстрируем выполнение найденных формул на простых примерах.

Пример 1. Рассмотрим следующую задачу:

$$\begin{cases} x_1 + 2x_2 + 3x_3 \rightarrow \max, \\ x_1 + 2x_2 + x_3 \leq 3, \\ x_1, x_2, x_3 \in \{0, 1, 2\}. \end{cases}$$

У этой задачи 11 допустимых решений: $V_b = \{(000), (001), (010), (011), (100), (101), (110), (002), (200), (102), (201)\}$.

Для нахождения V_b вычислим $|V_b^{0k}|$ для наименьшего $a_k = 1$: $V_b^{01} = \{(00), (01), (10), (11), (02)\}$ — решения неравенства $2x_2 + x_3 \leq 3$, $|V_b^{01}| = 5$.

Далее для нахождения $\mu(\xi)$ вычислим $|V_b^{ik}|$ для $k = 1, 2, 3$, $i = 1, 2$ по формуле (13):

$V_b^{11} = \{(00), (10), (01), (02)\}$ — решения неравенства $2x_2 + x_3 \leq 2$, $|V_b^{11}| = 4$;

$V_b^{21} = \{(00), (01)\}$ — решения неравенства $2x_2 + x_3 \leq 1$, $|V_b^{21}| = 2$;

$V_b^{12} = \{(00), (01), (10)\}$ — решения неравенства $x_1 + x_3 \leq 1$, $|V_b^{12}| = 3$;

$V_b^{22} = \emptyset$ — решения неравенства $x_1 + x_3 \leq -1$, $|V_b^{22}| = 0$;

$V_b^{13} = \{(00), (01), (10), (20)\}$ — решения неравенства $x_1 + 2x_2 \leq 2$, $|V_b^{13}| = 4$;

$V_b^{23} = \{(00), (10)\}$ — решения неравенства $x_1 + 2x_2 \leq 1$, $|V_b^{23}| = 2$.

Подставляя эти значения в (16) и (14), получаем

$$|V_b| = |V_b^{01}| + |V_b^{11}| + |V_b^{21}| = 5 + 4 + 2 = 11,$$

$$\mu(\xi) = \sum_{k=1}^n c_k \left(\frac{|V_b^{1k}|}{|V_b|} + 2 \frac{|V_b^{2k}|}{|V_b|} \right) = 1 \left(\frac{4}{11} + 2 \cdot \frac{2 \cdot 2}{11} \right) + 2 \left(\frac{3}{11} + \frac{2 \cdot 0}{11} \right) + 3 \left(\frac{4}{11} + \frac{2 \cdot 2}{11} \right) = \frac{38}{11}.$$

Это соответствует значению математического ожидания функционала задачи при прямом подсчёте:

$$\mu(\xi) = \frac{1}{11} (0 + 1 + 2 + 3 + 5 + 4 + 3 + 6 + 2 + 7 + 5) = \frac{38}{11}.$$

Как видно из примера, приведённые в теореме 1 формулы позволяют декомпозировать задачу на подзадачи меньшей размерности, в которых значение ограничения b меньше исходного.

Пример 2. Рассмотрим следующую задачу:

$$\begin{cases} x_1 + 2x_2 + 3x_3 + 4x_4 \rightarrow \max, \\ 2x_1 + 3x_2 + 4x_3 + 6x_4 \leq 6, \\ x_1, x_2, x_3, x_4 \in \{0, 1, 2, 3\}. \end{cases}$$

У этой задачи 10 допустимых решений: $\{(0000), (0001), (0010), (0100), (0200), (1000), (1010), (1100), (2000), (3000)\}$.

По формуле (13) получим

$$|V_b^{01}| = 5, \quad |V_b^{11}| = 3, \quad |V_b^{21}| = 1, \quad |V_b^{31}| = 1, \quad |V_b^{12}| = 2, \quad |V_b^{22}| = 1, \quad |V_b^{32}| = 0,$$

$$|V_b^{13}| = 2, \quad |V_b^{23}| = 0, \quad |V_b^{33}| = 0, \quad |V_b^{14}| = 2, \quad |V_b^{24}| = 0, \quad |V_b^{34}| = 0.$$

Подставляя эти значения в (16) для $k = 1$, находим число решений исходной задачи:

$$|V_b| = |V_b^{01}| + |V_b^{11}| + |V_b^{21}| + |V_b^{31}| = 5 + 3 + 1 + 1 = 10.$$

Подставляя все найденные значения в (14), находим среднее значение функционала:

$$\begin{aligned}\mu(\xi) &= \sum_{k=1}^n c_k \left(\frac{|V_b^{1k}|}{|V_b|} + 2 \frac{|V_b^{2k}|}{|V_b|} + 3 \frac{|V_b^{3k}|}{|V_b|} \right) = \\ &= 2 \frac{3 + 2 \cdot 1 + 3 \cdot 1}{10} + 3 \frac{2 + 2 \cdot 1 + 3 \cdot 0}{10} + 4 \frac{2 + 2 \cdot 0 + 3 \cdot 0}{10} + 6 \frac{2 + 2 \cdot 0 + 3 \cdot 0}{10} = \frac{48}{13}.\end{aligned}$$

Это соответствует решению, полученному прямой подстановкой:

$$\mu(\xi) = \frac{1}{13} (0 + 4 + 2 + 6 + 4 + 1 + 5 + 3 + 5 + 2 + 6 + 4 + 6) = \frac{48}{13}.$$

Как показывают приведённые примеры, большинство членов в формуле (14) равны нулю, что уменьшает количество необходимых для вычислений значений.

Пример 3. Пусть $a_i = 2^{i-1}$ для всех $i = 1, 2, \dots, n$, а $b = 2^{n+1}$, тогда решения неравенства $\sum_{i=1}^n a_i x_i \leq b$, $x_i \in \{0, 1, 2\}$ — это все элементы пространства n -мерных векторов с координатами из $\{0, 1, 2\}$. Получаем $|V_b| = 3^n$.

Для любого k находим решения неравенства $\sum_{i=1, i \neq k}^n a_i x_i \leq b - a_k$, $x_i \in \{0, 1, 2\}$.

Это все элементы пространства $(n-1)$ -мерных векторов с координатами из $\{0, 1, 2\}$, поэтому $|V_b^{1k}| = 3^{n-1}$. Рассуждая аналогично, получаем $|V_b^{2k}| = 3^{n-1}$. Отсюда среднее значение $\mu(\xi) = \sum_{k=1}^n c_k (1/3 + 2/3) = \sum_{k=1}^n c_k$, а максимальное значение функционала равно $\sum_{k=1}^n 2c_k$.

3. Сюръективность в задаче о рюкзаке

Рассмотрим случай, при котором коэффициенты целевой функции и векторы ограничений совпадают, т. е. $a_i = c_i$, $i = 1, \dots, n$.

Определение 1. Пусть $M = \{0, 1, \dots, m\}$; M^n — множество всех n -мерных векторов с координатами из M . Назовём функцию $f(x_1, \dots, x_n) = \sum_{j=1}^n c_j x_j$ сюръективной на множестве $N \subset M^n$, если она принимает на N все значения из интервала $[f_{\min}, \dots, f_{\max}]$, где f_{\min}, f_{\max} — минимальное и максимальное значение данной функции на множестве N .

Ранее определение линейной функции с булевыми переменными $f(x_1, \dots, x_n) = \sum_{j=1}^n c_j x_j$, принимающей все значения из интервала $[0, \sum_{j=1}^n c_j]$, было дано, например, в работе [22]. Подробный анализ свойств таких функций приведён в [23].

Примерами сюръективных функций на всём M^n при любом m являются: $f(x_1, \dots, x_n) = \sum_{j=1}^n 2^{j-1} x_j$; $f(x_1, \dots, x_n) = \sum_{j=1}^n j x_j$. Функция $2x_1 + 3x_2 + 4x_3$ при любом m не является сюръективной, поскольку она не принимает значение 1.

Теорема 2. Если $f(x_1, \dots, x_n) = \sum_{j=1}^n c_j x_j$ — сюръективная функция на V_b , где $x_i \in \{0, 1, \dots, m\}$, $i = 1, \dots, n$, то

$$(m+1)^n - 1 \geq \max f(x_1, \dots, x_n) \geq \sum_{k=1}^n c_k \left(\frac{|V_b^{1k}|}{|V_b|} + 2 \frac{|V_b^{2k}|}{|V_b|} + \dots + m \frac{|V_b^{mk}|}{|V_b|} \right).$$

Доказательство. Пусть $C = \{c_1, c_2, \dots, c_n\}$ и $S(C, n)$ — число различных сумм из элементов C . Очевидно, что $S(C, n) \leq (m+1)^n - 1$. Наименьшее значение $f(x_1, \dots, x_n)$ равно нулю. Поскольку функция $f(x_1, \dots, x_n)$ сюръективная, она должна принимать все значения, начиная с нуля, поэтому её максимальное значение не может превосходить числа $S(C, n)$:

$$(m+1)^n - 1 \leq \max f(x_1, \dots, x_n).$$

Нижняя оценка следует из теоремы 1. ■

Пример 4. Верхняя оценка из теоремы 2 достигается для произвольного m при $c_i = (m+1)^{i-1}$, $i = 1, \dots, n$, и $b \leq \sum_{j=1}^n c_j$. В этом случае $S(C, n) = (m+1)^n - 1$ и $f(x_1, \dots, x_n) = \sum_{j=1}^n c_j x_j$ — сюръективная функция с максимальным значением $(m+1)^n - 1$.

Заключение

Рассмотрены вопросы, связанные с вычислением и оценкой значений функционала задачи об ограниченном рюкзаке. Приведены формулы и оценки числа допустимых решений задачи в зависимости от числа решений подзадач меньшей размерности. Метод производящих функций может быть успешно применён для анализа подобных задач, имеющих комбинаторную природу. Полученные формулы могут быть уточнены при рассмотрении задач специального вида, которые возникают в конкретных прикладных областях, в частности в математических моделях информационной безопасности, учитывающих реальные особенности исходных постановок. Изложенные результаты могут послужить базой для дальнейших исследований свойств структуры многогранников задач о рюкзаке. Найденные выражения могут быть также использованы непосредственно в вычислительных алгоритмах в качестве вспомогательных процедур.

ЛИТЕРАТУРА

1. Kellerer H., Pferschy U., and Pisinger D. Knapsack Problems. Berlin: Springer, 2004. 548 p.
2. Егорычев Г. П. Интегральное представление и вычисление комбинаторных сумм. Новосибирск: Наука, 1977. 285 с.
3. Zhang H., Han W., Lai X., et al. Survey on cyberspace security // Sci. China Inform. Sci. 2015. V. 58. No. 11. P. 1–43.
4. Lyubashevsky V., Palacio A., and Segev G. Public-key cryptographic primitives provably as secure as subset sum // LNCS. 2010. V. 5978. P. 382–400.
5. Ranjith J. and Mahantesh K. Blockchain-based knapsack system for security and privacy preserving to medical data // SN Comput. Sci. 2021. V. 2. <https://www.researcher-app.com/paper/7553542>.
6. Martello S. and Toth P. Knapsack Problems: Algorithms and Computer Implementations. N.Y.: John Wiley & Sons, 1990. 308 p.
7. Zhang X., Huang S., Hu Y., et al. Solving 0-1 knapsack problems based on amoeboid organism algorithm // Appl. Math. Comput. 2013. V. 219. No. 19. P. 9959–9970.
8. Kulkarni A. J. and Shabir H. Solving 0-1 knapsack problem using Cohort Intelligence Algorithm // Int. J. Mach. Learn. & Cyber. 2014. V. 7. P. 427–441.
9. Rezoug A., Bader-El-Den M., and Boughaci D. Guided genetic algorithm for the multi-dimensional knapsack problem // Memetic Computing. 2018. V. 10. P. 29–42.

10. Kong X., Gao L., Ouyang H., and Li S. Solving large-scale multidimensional knapsack problems with a new binary harmony search algorithm // Computers & Operations Res. 2015. V. 63. P. 7–22.
11. Lv J., Wang X., Huang M., et al. Solving 0-1 knapsack problem by greedy degree and expectation efficiency // Appl. Soft Comput. 2016. V. 41. P. 94–103.
12. Chen Y. and Hao J.-K. A “reduce and solve” approach for the multiple-choice multidimensional knapsack problem // Europ. J. Operational Res. 2014. V. 239. No. 2. P. 312–322.
13. Voß S. and Lalla-Ruiz E. A set partitioning reformulation for the multiple-choice multidimensional knapsack problem // Engin. Optimization. 2016. V. 48. No. 5. P. 831–850.
14. Dang C. and Ye Y. A fixed point iterative approach to integer programming and its distributed computation // Fixed Point Theory Appl. 2015. <https://fixedpointtheoryandalgorithms.springeropen.com/articles/10.1186/s13663-015-0429-8>.
15. Pesant G. Counting solutions of CSPs: A structural approach // Proc. IJCAI'05. Edinburgh, Scotland, 2005. P. 260–265.
16. Louveaux Q. and Weismantel R. Polyhedral properties for the intersection of two knapsacks // Math. Program. 2008. V. 113. P. 15–37.
17. Hojny C., Gally T., Habeck O., et al. Knapsack polytopes: a survey // Ann. Oper. Res. 2020. V. 292. P. 469–517.
18. Леонтьев В. К., Гордеев Э. Н. Производящие функции в задаче о ранце // Доклады Академии наук. 2018. Т. 481. № 5. С. 478–480.
19. Гордеев Э. Н., Леонтьев В. К. О некоторых комбинаторных свойствах задачи о рюкзаке // Ж. вычисл. матем. и матем. физ. 2019. Т. 59. № 8. С. 1439–1447.
20. Леонтьев В. К., Гордеев Э. Н. О числе решений системы булевых уравнений // Автоматика и телемеханика. 2021. № 9. С. 150–168.
21. Леонтьев В. К., Гордеев Э. Н. О некоторых особенностях задачи разрешимости систем булевых уравнений // Вопросы кибербезопасности. 2021. № 1(41). С. 18–28.
22. Леонтьев В. К. О псевдобулевых полиномах // Ж. вычисл. матем. и матем. физ. 2015. Т. 55. № 11. С. 1952–1958.
23. Леонтьев В. К., Гордеев Э. Н., Волков М. С. А. Классическая непрерывность и ее дискретный вариант // Прикладная физика и математика. 2022. № 1. С. 31–37.

REFERENCES

1. Kellerer H., Pferschy U., and Pisinger D. Knapsack Problems. Berlin, Springer, 2004. 548 p.
2. Egorychev G. P. Integral'noe predstavlenie i vychislenie kombinatornykh summ [Integral Representation and the Computation of Combinatorial Sums]. Novosibirsk, Nauka, 1977. 285 p. (in Russian)
3. Zhang H., Han W., Lai X., et al. Survey on cyberspace security. Sci. China Inform. Sci., 2015. vol. 58, no. 11, pp. 1–43.
4. Lyubashevsky V., Palacio A., and Segev G. Public-key cryptographic primitives provably as secure as subset sum. LNCS, 2010, vol. 5978, pp. 382–400.
5. Ranjith J. and Mahantesh K. Blockchain-based knapsack system for security and privacy preserving to medical data. // SN Comput. Sci., 2021, vol. 2, <https://www.researcher-app.com/paper/7553542>.
6. Martello S. and Toth P. Knapsack Problems: Algorithms and Computer Implementations. N.Y., John Wiley & Sons, 1990. 308 p.
7. Zhang X., Huang S., Hu Y., et al. Solving 0-1 knapsack problems based on amoeboid organism algorithm. Appl. Math. Comput., 2013, vol. 219, no. 19, pp. 9959–9970.

8. *Kulkarni A. J. and Shabir H.* Solving 0-1 knapsack problem using Cohort Intelligence Algorithm. *Int. J. Mach. Learn. & Cyber.*, 2014, vol. 7, pp. 427–441.
9. *Rezoug A., Bader-El-Den M., and Boughaci D.* Guided genetic algorithm for the multi-dimensional knapsack problem. *Memetic Computing*, 2018, vol. 10, pp. 29–42.
10. *Kong X., Gao L., Ouyang H., and Li S.* Solving large-scale multidimensional knapsack problems with a new binary harmony search algorithm. *Computers & Operations Res.*, 2015, vol. 63, pp. 7–22.
11. *Lv J., Wang X., Huang M., et al.* Solving 0-1 knapsack problem by greedy degree and expectation efficiency. *Appl. Soft Comput.*, 2016, vol. 41, pp. 94–103.
12. *Chen Y. and Hao J.-K.* A “reduce and solve” approach for the multiple-choice multidimensional knapsack problem. *Europ. J. Operational Res.*, 2014, vol. 239, no. 2, pp. 312–322.
13. *Voß S. and Lalla-Ruiz E.* A set partitioning reformulation for the multiple-choice multidimensional knapsack problem. *Engin. Optimization*, 2016, vol. 48, no. 5, pp. 831–850.
14. *Dang C. and Ye Y.* A fixed point iterative approach to integer programming and its distributed computation. *Fixed Point Theory Appl.*, 2015, <https://fixedpointtheoryandalgorithms.springeropen.com/articles/10.1186/s13663-015-0429-8>.
15. *Pesant G.* Counting solutions of CSPs: A structural approach, *Proc. IJCAI'05*, Edinburgh, Scotland, 2005, pp. 260–265.
16. *Louveaux Q. and Weismantel R.* Polyhedral properties for the intersection of two knapsacks. *Math. Program.*, 2008, vol. 113, pp. 15–37.
17. *Hojny C., Gally T., Habeck O., et al.* Knapsack polytopes: a survey. *Ann. Oper. Res.*, 2020, vol. 292, pp. 469–517.
18. *Leont'ev V. K. and Gordeev E. N.* Proizvodyashchie funktsii v zadache o rantse [The generating functions in the knapsack problem]. *Doklady Akademii Nauk*, 2018, vol. 481, no. 5, pp. 478–480. (in Russian)
19. *Gordeev E. N. and Leont'ev V. K.* On combinatorial properties of the knapsack problem. *Comput. Math. Math. Phys.*, 2019, vol. 59, no. 8, pp. 1380–1388.
20. *Leontiev V. K. and Gordeev E. N.* On the number of solutions to a system of Boolean equations. *Autom. Remote Control*, 2021, vol. 82, no. 9, pp. 1581–1596.
21. *Leont'ev V. K. and Gordeev E. N.* O nekotorykh osobennostyakh zadachi razreshimosti sistem bulevykh uravneniy [On some features of the problem of solvability of Boolean equations systems]. *Voprosy Kiberbezopasnosti*, 2021, no. 1(41), pp. 18–28. (in Russian)
22. *Leontiev V. K.* On pseudo-Boolean polynomials. // *Comput. Math. Math. Phys.*, 2015, vol. 55, no. 11, pp. 1926–1932.
23. *Leont'ev V. K., Gordeev E. N., and Volkov M. S. A.* Klassicheskaya nepreryvnost' i ee diskretnyy variant [Classical continuity and its discrete variant]. *Prikladnaya Fizika i Matematika*, 2022, no. 1, pp. 31–37. (in Russian)