2013 Вычислительные методы в дискретной математике №2(20)
DOI 10.17223/20710410/20/10
УДК 511

МОДИФИКАЦИЯ МЕТОДА ЛАГАРИАСА — ОДЛЫЖКО ДЛЯ РЕШЕНИЯ ОБОБЩЁННОЙ ЗАДАЧИ О РЮКЗАКЕ И СИСТЕМ ЗАДАЧ О РЮКЗАКАХ

Д. М. Мурин

Ярославский государственный университет им. П. Г. Демидова, г. Ярославль, Россия

E-mail: nirum87@mail.ru

В работе 1985 г. Дж. Лагариас и А. Одлыжко предложили метод решения вычислительной задачи о рюкзаке, основанный на её сведении к задаче поиска короткого вектора в решётке специального вида. Метод Лагариаса — Одлыжко позволяет решать «практически все» задачи о рюкзаках, обладающие малой плотностью. В настоящей работе метод Лагариаса — Одлыжко решения задачи о рюкзаке модифицируется применительно к случаям обобщённой задачи о рюкзаке и систем задач о рюкзаках. Система задач о рюкзаках вводится в настоящей работе как конечное множество индивидуальных задач о рюкзаках, имеющих общее решение. Определяются множества значений плотности обобщённых задач о рюкзаках и систем задач о рюкзаках, такие, что модифицированные методы позволяют решать «практически все» обобщённые задачи о рюкзаках и системы задач о рюкзаках, обладающие плотностью из этих множеств.

Ключевые слова: *метод Лагариаса — Одлыжко, задача о рюкзаке, обобщённая задача о рюкзаке, системы задач о рюкзаках.*

Введение

Задача о рюкзаке (распознавания) NP-полна [1]. Однако на настоящий момент известны два метода решения вычислительных задач о рюкзаках, обладающих малой плотностью, один из которых предложен Дж. Лагариасом и А. Одлыжко [2], а второй — Э. Брикеллом [3]. Дж. Лагариас и А. Одлыжко рассматривали *вычислительную задачу о рюкзаке* в следующей формулировке.

Условие: заданы вектор $A = (a_1, a_2, \ldots, a_r) \in \mathbb{N}^r$ и число $S \in \mathbb{N}$, причём известно, что уравнение

$$\sum_{i=1}^{r} a_i x_i = S, \tag{1}$$

где $x_1, \ldots, x_r$ — неизвестные, имеет решение в числах 0 и 1.

Вопрос: найти решение уравнения (1) в числах 0 и 1.

В работе [2] рассматривается понятие *плотности* задачи о рюкзаке.

Определение 1. *Плотностью* задачи о рюкзаке с вектором $A = (a_1, a_2, \ldots, a_r) \in \mathbb{N}^r$ называется число

$$d_{\text{з.р}} = \frac{r}{\log_2 \left(\max\limits_{1 \leqslant i \leqslant r} a_i \right)}.$$

Метод Лагариаса — Одлыжко основан на сведении задачи о рюкзаке к задаче поиска короткого вектора в решётке специального вида. Предположим, что имеется алгоритм «Оракул», который за полиномиальное время выдаёт один из кратчайших (самых коротких) ненулевых векторов решёток некоторых специальных видов (виды

решёток описаны далее). Несмотря на то, что задача нахождения кратчайшего ненулевого вектора решётки в общем случае является NP-трудной [4], ответ на вопрос о существовании алгоритма «Оракул» неизвестен, при реализации «приближением» к этому алгоритму служит алгоритм построения LLL-приведённого базиса решётки.

Дж. Лагариас и А. Одлыжко рассматривали решётку $\Lambda_1 = \{z_1 b_1 + \ldots + z_{r+1} b_{r+1} : z_1, \ldots, z_{r+1} \in \mathbb{Z}\}$, образованную следующими линейно независимыми векторами размерности $r+1$:

$$\begin{gathered} b_1 = (1, 0, \ldots, 0, N \cdot a_1), \\ b_2 = (0, 1, \ldots, 0, N \cdot a_2), \\ \vdots \\ b_r = (0, 0, \ldots, 1, N \cdot a_r), \\ b_{r+1} = (0, 0, \ldots, 0, N \cdot S), \end{gathered}$$

где $N \geqslant \left[\sqrt{r/2}\right] + 1$ — некоторое достаточно большое натуральное число, а вектор $(a_1, \ldots, a_r, S) \in \mathbb{N}^{r+1}$ задаёт вычислительную задачу о рюкзаке. В работе [2] показано, что справедлива следующая теорема.

Теорема 1. Пусть $a_1, \ldots, a_r$ — произвольные натуральные числа, $\tilde{e} = (e_1, \ldots, e_r) \in \in \{0,1\}^r$ — произвольный вектор и $S = \sum\limits_{i=1}^{r} e_i a_i$. Тогда вероятность ошибки при решении задачи о рюкзаке, заданной значениями a_i, $1 \leqslant i \leqslant r$, и S, при условии, что плотность этой задачи $d_{\text{з.р}} < 0{,}6463\ldots$, с помощью алгоритма «Оракул», применённого к решётке Λ_1, стремится к 0 при $r \to \infty$. (Здесь и далее под ошибкой понимается получение с помощью «Оракула» вектора, отличного от $\tilde{e}$ и $-\tilde{e}$.)

Этот результат улучшен в работе [5] путём модификации исследуемой решётки. Определим решётку $\Lambda_2 = \{z_1 b_1^* + \ldots + z_{r+1} b_{r+1}^* : z_1, \ldots, z_{r+1} \in \mathbb{Z}\}$, где $b_i^* = b_i$ при $1 \leqslant i \leqslant r$ и $b_{r+1}^* = (1/2, 1/2, \ldots, 1/2, N \cdot S)$, $N \geqslant \left[\sqrt{r}/2\right] + 1$ — некоторое достаточно большое натуральное число. Заметим, что в данном случае векторы $b_1^*, \ldots, b_{r+1}^*$ не обязательно линейно независимы.

Справедлива следующая теорема [5].

Теорема 2. Пусть $a_1, \ldots, a_r$ — произвольные натуральные числа, $\tilde{e} = (e_1, \ldots, e_r) \in \in \{0,1\}^r$ — произвольный вектор и $S = \sum\limits_{i=1}^{r} e_i a_i$. Тогда вероятность ошибки при решении задачи о рюкзаке, заданной значениями a_i, $1 \leqslant i \leqslant r$, и S, при условии, что плотность этой задачи $d_{\text{з.р}} < 0{,}9408\ldots$, с помощью алгоритма «Оракул», применённого к решётке Λ_2, стремится к 0 при $r \to \infty$.

В настоящей работе предлагаются методы решения вычислительной обобщённой задачи о рюкзаке и систем задач о рюкзаках, основанные на методе Лагариаса — Одлыжко решения вычислительной задачи о рюкзаке.

Вычислительная обобщённая задача о рюкзаке рассматривается в следующей формулировке.

Условие: заданы вектор $A = (a_1, a_2, \ldots, a_r) \in \mathbb{N}^r$, число $S \in \mathbb{N}$ и натуральное число $m \geqslant 2$, причём известно, что уравнение

$$\sum_{i=1}^{r} a_i x_i = S, \tag{2}$$

где $x_1, \ldots, x_r$ — неизвестные, имеет решение в числах $0, 1, \ldots, m-1$.

Вопрос: найти решение уравнения (2) в числах $0, 1, \ldots, m-1$.

Замечание. Числа $0, 1, \ldots, m-1$ можно рассматривать как элементы кольца вычетов $\mathbb{Z}/m\mathbb{Z}$, но поскольку в обобщённой задаче о рюкзаке рассматривается обычная сумма $\sum\limits_{i=1}^{r} a_i x_i$ натуральных чисел, то оперирование значениями $0, 1, \ldots, m-1$ представляется более естественным.

Определение 2. *Плотностью* обобщённой задачи о рюкзаке с вектором $A = (a_1, a_2, \ldots, a_r) \in \mathbb{N}^r$ назовём число

$$d_{\text{о.з.р}} = \frac{r}{\log_m \left(\max\limits_{1 \leqslant i \leqslant r} a_i \right)}.$$

Системой задач о рюкзаках назовём конечное множество индивидуальных задач о рюкзаках, имеющих общее решение. Таким образом, система задач о рюкзаках является естественным обобщением индивидуальной задачи о рюкзаке. Кроме того, с точки зрения информационной безопасности система задач о рюкзаках тесно связана со случаем широковещательной рассылки сообщения, например в криптосистеме Меркля — Хеллмана. Дадим строгую формулировку *системы обобщённых задач о рюкзаках.*

Условие: заданы k векторов $A_1 = (a_{11}, \ldots, a_{r1})$, $\ldots$, $A_k = (a_{1k}, \ldots, a_{rk})$ размерности r, k натуральных чисел $S_1, \ldots, S_k$ и натуральное число $m \geqslant 2$, причём известно, что система уравнений

$$\sum_{i=1}^{r} a_{ij} x_i = S_j, \quad 1 \leqslant j \leqslant k, \tag{3}$$

где $x_1, \ldots, x_r$ — неизвестные, имеет решение в числах $0, 1, \ldots, m-1$.

Вопрос: найти решение системы уравнений (3) в числах $0, 1, \ldots, m-1$.

Определение 3. *Плотностью* системы обобщённых задач о рюкзаках с векторами $A_1 = (a_{11}, \ldots, a_{r1})$, $\ldots$, $A_k = (a_{1k}, \ldots, a_{rk})$ назовём число

$$d_{\text{с.о.з.р}} = \frac{r}{\log_m \left(\max\limits_{1 \leqslant i \leqslant r, 1 \leqslant j \leqslant k} a_{ij} \right)}.$$

Обозначим через $S_r(R)$ число точек целочисленной решётки, попавших внутрь или на поверхность r-мерной сферы радиуса $\sqrt{R}$ с центром в начале координат (в r-мерном пространстве). В работе [2], по существу, доказана следующая теорема (непосредственно в работе рассматривался случай $m = 2$), необходимая нам для получения основных результатов.

Теорема 3. Для всех $\alpha > 0$, натуральных чисел $r \geqslant 1$ и любого натурального числа $m \geqslant 2$

$$S_r(\alpha r) \leqslant e^{\gamma} = m^{\gamma \log_m e},$$

где $\gamma = \min\limits_{x \geqslant 0} \delta(\alpha, x) \cdot r$; $\delta(\alpha, x) = \alpha x + \ln \theta(e^{-x})$; $\theta(z) = 1 + 2 \sum\limits_{i=1}^{\infty} z^{i^2}$.

1. Модификация метода Лагариаса — Одлыжко для случая обобщённой задачи о рюкзаке

Рассмотрим решётку Λ_3, образованную следующими векторами $b_1, \ldots, b_{r+1}$ размерности $r+1$:

$$\begin{gathered} b_1 = (1, 0, \ldots, 0, N \cdot a_1), \\ b_2 = (0, 1, \ldots, 0, N \cdot a_2), \\ \vdots \\ b_r = (0, 0, \ldots, 1, N \cdot a_r), \\ b_{r+1} = (0, 0, \ldots, 0, N \cdot S), \end{gathered}$$

где $N \geqslant \left[(m-1)\sqrt{r/2}\right] + 1$ — некоторое достаточно большое натуральное число.

Определение 4. Назовем обобщённую задачу о рюкзаке *приведённой*, если выполнены неравенства

$$\frac{1}{r}\sum_{i=1}^{r} a_i \leqslant S \leqslant (m-1)\sum_{i=1}^{r} a_i - \frac{1}{r}\sum_{i=1}^{r} a_i.$$

Если обобщённая задача о рюкзаке не является приведённой, то имеется возможность исключить из рассмотрения либо самый большой (если $\frac{1}{r}\sum\limits_{i=1}^{r} a_i \geqslant S$), либо самый маленький (если $S \geqslant (m-1)\sum\limits_{i=1}^{r} a_i - \frac{1}{r}\sum\limits_{i=1}^{r} a_i$) элемент вектора. Для приведённой обобщённой задачи о рюкзаке такой возможности нет.

Для любого натурального числа $m \geqslant 2$ справедлива следующая теорема.

Теорема 4. Пусть $a_1, \ldots, a_r$ — произвольные натуральные числа, $\tilde{e} = (e_1, \ldots, e_r) \in \{0, 1, \ldots, m-1\}^r$ — произвольный вектор и $S = \sum\limits_{i=1}^{r} e_i a_i$. Тогда вероятность ошибки при решении приведённой обобщённой задачи о рюкзаке, заданной значениями a_i, $1 \leqslant i \leqslant r$, и S, при условии, что плотность этой задачи $d_{\text{о.з.р}} < \dfrac{\ln m}{\min\limits_{x \geqslant 0} \delta((m-1)^2/2, x)}$, с помощью алгоритма «Оракул», применённого к решетке Λ_3, стремится к 0 при $r \to \infty$.

Доказательство. Решётка Λ_3 содержит вектор $e = (e_1, e_2, \ldots, e_r, 0)$, где $e_1, \ldots, e_r$ — решение ассоциированной обобщённой задачи о рюкзаке ($e = \sum\limits_{i=1}^{r} e_i b_i - b_{r+1}$).

Пусть $t = \sum\limits_{i=1}^{r} a_i$. Можно считать, что $\sum\limits_{i=1}^{r} e_i \leqslant (m-1)r/2$, иначе можно перейти к «дополняющей» задаче со следующими параметрами:

$$\begin{gathered} S^{\text{new}} = (m-1)t - S, \\ b_{r+1}^{\text{new}} = (0, 0, \ldots, 0, N((m-1)t - S)), \\ e^{\text{new}} = (m-1-e_1, m-1-e_2, \ldots, m-1-e_r, 0). \end{gathered}$$

Решение «дополняющей» задачи эквивалентно решению исходной задачи, при этом $\sum\limits_{i=1}^{r}(m-1-e_i) \leqslant (m-1)r/2$ (заметим также, что $S^{\text{new}} = (m-1)t - S \geqslant (m-1)t - -(m-1)t + t/r = t/r$).

Поскольку $\sum\limits_{i=1}^{r} e_i \leqslant (m-1)r/2$, $e_i \in \{0, 1, \ldots, m-1\}$ и $h^2 + (m-1-h)^2 \leqslant (m-1)^2$ при $0 \leqslant h \leqslant m-1$, то $||e||^2 = \sum\limits_{i=1}^{r} e_i^2 \leqslant (m-1)^2 r/2$.

Поэтому вектор e является «*достаточно коротким*» вектором решётки и его можно искать при помощи «Оракула». Однако может оказаться, что «Оракул» выдаст вектор, не совпадающий с векторами $-e, e$. В этом случае вектор, предоставленный «Оракулом», является элементом следующего множества ошибочных векторов:

$$X_3 = \{x = (x_1, \ldots, x_{r+1}) : x \in \Lambda_3, ||x|| \leqslant ||e||, x \notin \{-e, 0, e\}\}.$$

Выбор числа $N \geqslant \left[(m-1)\sqrt{r/2}\right] + 1$ обеспечивает для векторов $x \in X_3$ выполнение условия $x_{r+1} = 0$ (иначе если $x \in X_3$ и $x_{r+1} \neq 0$, то $||x|| \geqslant |x_{r+1}| \geqslant N > (m-1)\sqrt{r/2} \geqslant$ $\geqslant ||e||$, то есть $x \notin X_3$ — противоречие).

Рассмотрим произвольный вектор $x \in X_3$ и определим число $y \in \mathbb{Z}$ следующим образом:

$$yS = \sum_{i=1}^{r} x_i a_i,$$

тогда

$$|y|S = \left|\sum_{i=1}^{r} x_i a_i\right| \leqslant ||x|| \sum_{i=1}^{r} a_i \leqslant (m-1)t\sqrt{r/2}$$

и, поскольку $t \leqslant Sr$, получим $|y| \leqslant (m-1)r\sqrt{r/2}$.

Пусть P — вероятность того, что множество X_3 не является пустым, тогда справедливо неравенство

$$P \leqslant \Pr\left(\sum_{i=1}^{r} x_i a_i = yS \mid x \in X_3, |y| \leqslant (m-1)r\sqrt{r/2}\right) \cdot |X_3| \cdot \left|\left\{y : |y| \leqslant (m-1)r\sqrt{r/2}\right\}\right|.$$

Определим вектор $z = (z_1, z_2, \ldots, z_r)$, где $z_i = x_i - ye_i$, $1 \leqslant i \leqslant r$. Случай $z = 0$ не рассматривается, поскольку при этом $||x|| = |y|||e||$, и так как $||x|| \leqslant ||e||$, то $|y| \leqslant 1$ и $x \in \{-e, 0, e\}$, а значит, $x \notin X_3$.

Пусть $B = \max\limits_{1 \leqslant i \leqslant r} a_i$, без ограничения общности будем считать, что $z_1 \neq 0$. Определим

$$z^* = -\sum_{i=2}^{r} \frac{a_i z_i}{z_1},$$

тогда

$$\Pr\left(\sum_{i=1}^{r} z_i a_i = 0\right) = \Pr(a_1 = z^*) = \sum_{j=1}^{B} \Pr(a_1 = z^* \mid z^* = j)\Pr(z^* = j) =$$
$$= \sum_{j=1}^{B} \Pr(a_1 = j)\Pr(z^* = j) = \sum_{j=1}^{B} \frac{1}{B}\Pr(z^* = j) \leqslant \frac{1}{B}.$$

Предыдущая оценка получена в предположении, что $z_1 \neq 0$, но на самом деле каждый элемент z_i при $1 \leqslant i \leqslant r$ может быть не равным нулю, поэтому

$$\Pr\left(\sum_{i=1}^{r} z_i a_i = 0\right) \leqslant \frac{r}{B}.$$

С учётом результата теоремы 3 при $\alpha = (m-1)^2/2$ получим

$$|X_3| \leqslant \left|\left\{\tilde{x} \in \mathbb{Z}^r : ||\tilde{x}|| \leqslant (m-1)\sqrt{r/2}\right\}\right| \leqslant m^{\min\limits_{x \geqslant 0} \delta((m-1)^2/2, x) r \log_m e}.$$

По свойствам модуля

$$\left|\left\{y : |y| \leqslant (m-1)r\sqrt{r/2}\right\}\right| \leqslant 2(m-1)r\sqrt{r/2} + 1.$$

Таким образом,

$$P \leqslant r\left(2(m-1)r\sqrt{r/2} + 1\right) \frac{m^{\min\limits_{x \geqslant 0} \delta((m-1)^2/2, x) r \log_m e}}{B},$$

и если $B = m^{C_m r}$, то при $C_m > \min\limits_{x \geqslant 0} \delta((m-1)^2/2, x) \log_m e$ получим $\lim\limits_{r \to \infty} P = 0$.

Если плотность обобщённой задачи о рюкзаке

$$d_{\text{о.з.р}} = \frac{r}{\log_m \left(\max\limits_{1 \leqslant i \leqslant r} a_i\right)} < \frac{\ln m}{\min\limits_{x \geqslant 0} \delta((m-1)^2/2, x)},$$

то $B = \max\limits_{1 \leqslant i \leqslant r} a_i > m^{\min\limits_{x \geqslant 0} \delta((m-1)^2/2, x) r \log_m e}$. ■

2. Модификация метода Лагариаса — Одлыжко для случая систем обобщённых задач о рюкзаках

Рассмотрим решётку Λ_4, образованную следующими векторами $b_1, \ldots, b_{r+1}$ размерности $r + k$:

$$\begin{gathered}
b_1 = (1, 0, \ldots, 0, N \cdot a_{11}, N \cdot a_{12}, \ldots, N \cdot a_{1k}), \\
b_2 = (0, 1, \ldots, 0, N \cdot a_{21}, N \cdot a_{22}, \ldots, N \cdot a_{2k}), \\
\vdots \\
b_r = (0, 0, \ldots, 1, N \cdot a_{r1}, N \cdot a_{r2}, \ldots, N \cdot a_{rk}), \\
b_{r+1} = (0, 0, \ldots, 0, N \cdot S_1, N \cdot S_2, \ldots, N \cdot S_k),
\end{gathered}$$

где $N \geqslant [(m-1)\sqrt{r/2}] + 1$ — некоторое достаточно большое натуральное число.

Определение 5. Назовём систему обобщённых задач о рюкзаках *приведённой*, если для всех $1 \leqslant j \leqslant k$ выполнены неравенства

$$\frac{1}{r}\sum_{i=1}^{r} a_{ij} \leqslant S_j \leqslant (m-1)\sum_{i=1}^{r} a_{ij} - \frac{1}{r}\sum_{i=1}^{r} a_{ij}.$$

Для любого натурального числа $m \geqslant 2$ справедлива следующая теорема.

Теорема 5. Пусть a_{ij}, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant k$, — произвольные натуральные числа, причём векторы $A_1 = (a_{11}, \ldots, a_{r1}), \ldots, A_k = (a_{1k}, \ldots, a_{rk})$ являются линейно независимыми. Пусть $\tilde{e} = (e_1, \ldots, e_r) \in \{0, 1, \ldots, m-1\}^r$ — произвольный вектор и $S_j = \sum\limits_{i=1}^{r} e_i a_{ij}$ для всех $1 \leqslant j \leqslant k$. Тогда вероятность ошибки при решении приведённой системы обобщённых задач о рюкзаках, заданной значениями a_{ij}, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant k$, и S_j, $1 \leqslant j \leqslant k$, при условии, что плотность этой системы $d_{\text{с.о.з.р}} < \dfrac{k \ln m}{\min\limits_{x \geqslant 0} \delta((m-1)^2/2, x)}$, с помощью алгоритма «Оракул», применённого к решётке Λ_4, стремится к 0 при $r \to \infty$.

Доказательство. Решётке Λ_4 принадлежит вектор $e = (e_1, \ldots, e_r, 0, \ldots, 0)$, где $e_1, \ldots, e_r$ — решение ассоциированной системы обобщённых задач о рюкзаках. Отметим, что, как и ранее, можно считать, что $||e||^2 \leqslant (m-1)^2 r/2$.

Множеством ошибочных векторов в этом случае является

$$X_4 = \{x = (x_1, \ldots, x_{r+1}) : x \in \Lambda_4, ||x|| \leqslant ||e||, x \notin \{-e, 0, e\}\}.$$

Выбор числа $N \geqslant \left[(m-1)\sqrt{r/2}\right] + 1$ обеспечивает выполнение для векторов $x \in X_4$ условия $x_{r+j} = 0$ для всех $1 \leqslant j \leqslant k$ (иначе если $x \in X_4$ и $x_{r+j} \neq 0$ для некоторого $1 \leqslant j \leqslant k$, то $||x|| \geqslant |x_{r+j}| \geqslant N > (m-1)\sqrt{r/2} \geqslant ||e||$, то есть $x \notin X_4$ — противоречие).

Пусть $t_j = \sum\limits_{i=1}^{r} a_{ij}$ для всех $1 \leqslant j \leqslant k$. Рассмотрим произвольный вектор $x \in X_4$ и определим число $y \in \mathbb{Z}$ следующим образом:

$$yS_j = \sum_{i=1}^{r} x_i a_{ij} \text{ для всех } 1 \leqslant j \leqslant k,$$

тогда для всех $1 \leqslant j \leqslant k$

$$|y| S_j = \left| \sum_{i=1}^{r} x_i a_{ij} \right| \leqslant ||x|| \sum_{i=1}^{r} a_{ij} \leqslant (m-1) t_j \sqrt{r/2},$$

и поскольку $t_j \leqslant S_j r$, получим

$$|y| \leqslant (m-1) r \sqrt{r/2};$$

более точную оценку может дать неравенство

$$|y| \leqslant (m-1) \min_{1 \leqslant j \leqslant k} \{t_j / S_j\} \sqrt{r/2}.$$

Пусть P — вероятность того, что множество X_4 не является пустым, тогда справедливо неравенство

$$P \leqslant \Pr\left(\sum_{i=1}^{r} x_i a_{i1} = yS_1, \ldots, \sum_{i=1}^{r} x_i a_{ik} = yS_k \mid x \in X_4, |y| \leqslant (m-1) r \sqrt{r/2} \right) \cdot |X_4| \times$$
$$\times |\{y : |y| \leqslant (m-1) r \sqrt{r/2}\}| = \prod_{j=1}^{k} \Pr\left(\sum_{i=1}^{r} x_i a_{ij} = yS_j \mid x \in X_4, |y| \leqslant (m-1) r \sqrt{r/2} \right) \times$$
$$\times |X_4| \cdot |\{y : |y| \leqslant (m-1) r \sqrt{r/2}\}|.$$

Пусть $B = \max\limits_{1 \leqslant i \leqslant r, 1 \leqslant j \leqslant k} a_{ij}$. Как и прежде, можно показать, что для всех $1 \leqslant j \leqslant k$

$$\Pr\left(\sum_{i=1}^{r} x_i a_{ij} = yS_j \right) \leqslant \frac{r}{B},$$
$$\left| \left\{ y : |y| \leqslant (m-1) r \sqrt{r/2} \right\} \right| \leqslant 2(m-1) r \sqrt{r/2} + 1,$$
$$|X_4| \leqslant |\{\tilde{x} \in \mathbb{Z}^r : ||\tilde{x}|| \leqslant (m-1)\sqrt{r/2}\}| \leqslant m^{\min\limits_{x \geqslant 0} \delta((m-1)^2/2, x) r \log_m e}.$$

Таким образом, в этом случае

$$P \leqslant r^k \left(2(m-1) r \sqrt{r/2} + 1 \right) \frac{m^{\min\limits_{x \geqslant 0} \delta((m-1)^2/2, x) r \log_m e}}{B^k},$$

и если $B = m^{C_m r/k}$, то при $C_m > \min\limits_{x \geqslant 0} \delta((m-1)^2/2, x) \log_m e$ получим $\lim\limits_{r \to \infty} P = 0$.

Если плотность системы обобщённых задач о рюкзаках

$$d_{\text{с.о.з.р}} = \frac{r}{\log_m \left(\max\limits_{1 \leqslant i \leqslant r, 1 \leqslant j \leqslant k} a_{ij} \right)} < \frac{k \ln m}{\min\limits_{x \geqslant 0} \delta((m-1)^2/2, x)},$$

то $B = \max\limits_{1 \leqslant i \leqslant r, 1 \leqslant j \leqslant k} a_{ij} > m^{\min\limits_{x \geqslant 0} \delta((m-1)^2/2, x) \frac{r}{k} \log_m e}$. ■

При $m = 2$ будем называть систему обобщённых задач о рюкзаках системой задач о рюкзаках. Далее в теореме 6 определяется множество значений плотности систем задач о рюкзаках, такое, что алгоритм «Оракул» позволяет решать «практически все» системы задач о рюкзаках, обладающих плотностью из этого множества.

Рассмотрим решётку Λ_5, образованную следующими векторами $b_1, \ldots, b_{r+1}$ размерности $r + k$:

$$\begin{gathered}
b_1 = (1, 0, \ldots, 0, N \cdot a_{11}, N \cdot a_{12}, \ldots, N \cdot a_{1k}), \\
b_2 = (0, 1, \ldots, 0, N \cdot a_{21}, N \cdot a_{22}, \ldots, N \cdot a_{2k}), \\
\vdots \\
b_r = (0, 0, \ldots, 1, N \cdot a_{r1}, N \cdot a_{r2}, \ldots, N \cdot a_{rk}), \\
b_{r+1} = \left(\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2}, N \cdot S_1, N \cdot S_2, \ldots, N \cdot S_k \right),
\end{gathered}$$

где $N \geqslant [\sqrt{r}/2] + 1$ — некоторое достаточно большое натуральное число.

Теорема 6. Пусть a_{ij}, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant k$, — произвольные натуральные числа, причём векторы $A_1 = (a_{11}, \ldots, a_{r1}), \ldots, A_k = (a_{1k}, \ldots, a_{rk})$ являются линейно независимыми. Пусть $\tilde{e} = (e_1, \ldots, e_r) \in \{0, 1\}^r$ — произвольный вектор и $S_j = \sum\limits_{i=1}^{r} e_i a_{ij}$ для всех $1 \leqslant j \leqslant k$. Тогда вероятность ошибки при решении системы задач о рюкзаках, заданной значениями a_{ij}, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant k$, и S_j, $1 \leqslant j \leqslant k$, при условии, что плотность этой системы $d_{\text{с.з.р}} < k \cdot 0{,}9408\ldots$, с помощью алгоритма «Оракул», применённого к решётке Λ_5, стремится к 0 при $r \to \infty$.

Доказательство. Решётке Λ_5 принадлежит вектор $e^* = (e_1^*, \ldots, e_r^*, 0, \ldots, 0)$, где $e_i^* = e_i - 1/2$, а $e_1, \ldots, e_r$ — решение ассоциированной системы задач о рюкзаках ($e^* = \sum\limits_{i=1}^{r} e_i b_i - b_{r+1}$). Заметим, что $||e^*||^2 = r/4$.

Множеством ошибочных векторов в этом случае является

$$X_5 = \{x = (x_1, \ldots, x_{r+1}) : x \in \Lambda_5, ||x|| \leqslant ||e^*||, x \notin \{-e^*, 0, e^*\}\}.$$

Выбор числа $N \geqslant [\sqrt{r}/2] + 1$ обеспечивает выполнение для векторов $x \in X_5$ условия $x_{r+j} = 0$ для всех $1 \leqslant j \leqslant k$ (иначе если $x \in X_5$ и $x_{r+j} \neq 0$ для некоторого $1 \leqslant j \leqslant k$, то $||x|| \geqslant |x_{r+j}| \geqslant N > \sqrt{r}/2 \geqslant ||e^*||$, то есть $x \notin X_5$ — противоречие).

Поскольку для векторов множества X_5, являющихся, по определению, векторами решётки Λ_5, выполнено

$$x = \sum_{i=1}^{r} y_i b_i + y b_{r+1}$$

для некоторых целых y и y_i, $1 \leqslant i \leqslant r$, то $x_i = y_i + y/2$ для всех $1 \leqslant i \leqslant r$ и $x_{r+j} = N\left(\sum\limits_{i=1}^{r} a_{ij}y_i + yS_j\right)$ для всех $1 \leqslant j \leqslant k$.

Пусть $t_j = \sum\limits_{i=1}^{r} a_{ij}$ для всех $1 \leqslant j \leqslant k$. Оценим значение $|y|$. Так как $x_{r+j} = 0$ для всех $1 \leqslant j \leqslant k$, то $\sum\limits_{i=1}^{r} a_{ij}y_i = -yS_j$ для всех $1 \leqslant j \leqslant k$, и, подставляя значения $y_i = x_i - y/2$, получим $\sum\limits_{i=1}^{r}(x_i - y/2)a_{ij} = -yS_j$ и $\sum\limits_{i=1}^{r} x_i a_{ij} = \dfrac{1}{2}y\sum\limits_{i=1}^{r} a_{ij} - yS_j = \dfrac{1}{2}yt_j - yS_j = \dfrac{1}{2}y(t_j - 2S_j)$, поэтому для всех $1 \leqslant j \leqslant k$ выполнено

$$|y(t_j - 2S_j)| = 2\left|\sum_{i=1}^{r} x_i a_{ij}\right| \leqslant 2||x||\sum_{i=1}^{r} a_{ij} \leqslant \max_{1\leqslant i\leqslant r} a_{ij} r\sqrt{r}.$$

Пусть числа $1 \leqslant I \leqslant r$ и $1 \leqslant J \leqslant k$ являются наименьшими индексами, такими, что $a_{IJ} = \max\limits_{1\leqslant i\leqslant r, 1\leqslant j\leqslant k} a_{ij}$, тогда можно считать, что $|t_J - 2S_J| \geqslant a_{IJ}/2$. Иначе (если $|t_J - 2S_J| < a_{IJ}/2$) возможны только два случая.

В первом случае $e_I = 1$, и, исключив из рассмотрения для всех $1 \leqslant j \leqslant k$ элементы a_{Ij}, перейдём к системе задач о рюкзаках, в которой для всех $1 \leqslant j \leqslant k$

$$S_j^{\text{new}} = S_j - a_{Ij}, \qquad t_j^{\text{new}} = t_j - a_{Ij},$$
$$|t_J^{\text{new}} - 2S_J^{\text{new}}| = |t_J - a_{IJ} - 2S_J + 2a_{IJ}| = |t_J - 2S_J + a_{IJ}| \geqslant \frac{1}{2}a_{IJ}.$$

Во втором случае $e_I = 0$, и, исключив из рассмотрения для всех $1 \leqslant j \leqslant k$ элементы a_{Ij}, перейдём к системе задач о рюкзаках, в которой для всех $1 \leqslant j \leqslant k$

$$S_j^{\text{new}} = S_j, \qquad t_j^{\text{new}} = t_j - a_{Ij},$$
$$|t_J^{\text{new}} - 2S_J^{\text{new}}| = |t_J - 2S_J - a_{IJ}| \geqslant \frac{1}{2}a_{IJ}.$$

Теперь, поскольку $|t_J - 2S_J| \geqslant \dfrac{1}{2}a_{IJ}$,

$$a_{IJ}r\sqrt{r} \geqslant |y(t_J - 2S_J)| = |y||t_J - 2S_J| \geqslant \frac{1}{2}a_{IJ}|y|.$$

Таким образом, $|y| \leqslant 2r\sqrt{r}$.

Пусть P — вероятность того, что множество X_5 не является пустым, тогда справедливо следующее неравенство:

$$P \leqslant \Pr\left(\sum_{i=1}^{r} x_i a_{i1} = \frac{1}{2}y(t_1 - 2S_1), \ldots, \sum_{i=1}^{r} x_i a_{ik} = \frac{1}{2}y(t_k - 2S_k) \mid x \in X_5, |y| \leqslant 2r\sqrt{r}\right) \times$$
$$\times|\{x : ||x|| \leqslant ||e^*||\}| \cdot |\{y : |y| \leqslant 2r\sqrt{r}\}| =$$
$$= \prod_{j=1}^{k} \Pr\left(\sum_{i=1}^{r} x_i a_{ij} = \frac{1}{2}y(t_j - 2S_j) \mid x \in X_5, |y| \leqslant 2r\sqrt{r}\right) \times$$
$$\times|\{x : ||x|| \leqslant ||e^*||\}| \cdot |\{y : |y| \leqslant 2r\sqrt{r}\}|.$$

По построению векторов $b_1, \ldots, b_{r+1}$ ввиду того, что $x = \sum\limits_{i=1}^{r} y_i b_i + yb_{r+1}$ и $x_{r+1} = 0$, имеет место

$$|\{x : ||x|| \leqslant \sqrt{r}/2\}| \leqslant |\{\tilde{x} \in \mathbb{Z}^r : ||\tilde{x}|| \leqslant \sqrt{r}/2\}| + |\{\tilde{x} \in \mathbb{Z}^r : ||\tilde{x} - (1/2, \ldots, 1/2)|| \leqslant \sqrt{r}/2\}|.$$

В последней сумме первое слагаемое соответствует случаям с чётными y, а второе — с нечётными.

Далее, $|\{\tilde{x} : \tilde{x} \in \mathbb{Z}^r, ||\tilde{x} - (1/2, \ldots, 1/2)|| \leqslant \sqrt{r}/2\}| = 2^r$. С учётом результата теоремы 3, при $\alpha = 1/4$ получим

$$|\{\tilde{x} \in \mathbb{Z}^r : ||\tilde{x}|| \leqslant \sqrt{r}/2\}| \leqslant 2^{\min\limits_{x \geqslant 0} \delta(1/4, x) r \log_2 e}.$$

Численно устанавливается, что $\min\limits_{x \geqslant 0} \delta(1/4, x) \log_2 e = 1{,}0628\ldots$ Следовательно, можно утверждать, что

$$|\{x : ||x|| \leqslant \sqrt{r}/2\}| \leqslant 2^{C_1 r} + 2^r,$$

где $C_1 = 1{,}0628\ldots$

Пусть $B = \max\limits_{1 \leqslant i \leqslant r, 1 \leqslant j \leqslant k} a_{ij}$. Как и прежде, можно показать, что для всех $1 \leqslant j \leqslant k$

$$\Pr\left(\sum_{i=1}^{r} x_i a_{ij} = \frac{1}{2} y(t_j - 2S_j)\right) \leqslant \frac{r}{B}, \quad |\{y : |y| \leqslant 2r\sqrt{r}\}| \leqslant 4r\sqrt{r} + 1.$$

Таким образом, в этом случае

$$P \leqslant r^k (4r\sqrt{r} + 1) \frac{2^{C_1 r} + 2^r}{B^k},$$

и если $B = 2^{Cr/k}$, то при $C > C_1$ получим, что $\lim\limits_{r \to \infty} P = 0$.

Если плотность системы задачи о рюкзаках

$$d_{\text{с.з.р}} = \frac{r}{\log_2 \left(\max\limits_{1 \leqslant i \leqslant r, 1 \leqslant j \leqslant k} a_{ij} \right)} < k \cdot 0{,}9408\ldots,$$

то $B = \max\limits_{1 \leqslant i \leqslant r, 1 \leqslant j \leqslant k} a_{ij} > 2^{C_1 r/k}$. ■

ЛИТЕРАТУРА

1. *Karp R. M.* Reducibility among combinatorial problems // Complexity of Computer Computations. Plenum Press, 1972. P. 85–103.
2. *Odlyzko A. M. and Lagarias J. C.* Solving low-density subset sum problems // J. Association for Computing Machinery. 1985. V. 32. No. 1. P. 229–246.
3. *Brickell E. F.* Solving low-density knapsacks // Advances in Cryptology. Proc. Crypto'83. Plenun Press, 1984. P. 25–37.
4. *Boas P.* Another NP-complete problem and the complexity of computing short vectors in a lattice // Tech. rep. 8104, University of Amsterdam, Department of Mathematics, Netherlands, 1981. 10 p.
5. *Coster M. J., Joux A., LaMacchia B. A., et al.* Improved low-density subset sum algorithms // Computational Complexity. 1992. No. 2. P. 111–128.