Р5-2010-44

В. А. Шлык*

ЗАДАЧИ РАСПОЗНАВАНИЯ НЕКОТОРЫХ КЛАССОВ РАЗБИЕНИЙ ЧИСЕЛ И ЧИСЛОВЫХ МУЛЬТИМНОЖЕСТВ

Направлено в журнал «Математические заметки»

---

*Институт математики НАН Белоруссии
E-mail: v.shlyk@gmail.com

Шлык В. А. Р5-2010-44
Задачи распознавания некоторых классов разбиений чисел
и числовых мультимножеств

В работе показано, что класс разбиений, непредставимых в виде выпуклой комбинации двух разбиений того же числа, совпадает с классом рюкзачных разбиений и с классом мультимножеств Сидона, включающим множества без сумм и стандартные множества Сидона. Доказано, что задача распознавания рюкзачных разбиений co-NP-полна и, следовательно, неразрешима за полиномиальное время, если верна гипотеза $P \neq NP$.

Работа выполнена в Лаборатории теоретической физики им. Н. Н. Боголюбова ОИЯИ.

Препринт Объединенного института ядерных исследований. Дубна, 2010

Shlyk V. A. P5-2010-44
Decision Problems for Some Classes of Integer Partitions
and Number Multisets

We show that the class of integer partitions that cannot be represented as convex combinations of two partitions of the same numbers coincides with the class of knapsack partitions and the class of Sidon multisets, which includes sum-free sets and standard Sidon sets. The decision problem for knapsack partitions is proved to be co-NP-complete and, therefore, cannot be solved in polynomial time unless $P = NP$.

The investigation has been performed at the Bogoliubov Laboratory of Theoretical Physics, JINR.

Preprint of the Joint Institute for Nuclear Research. Dubna, 2010

ВВЕДЕНИЕ

Трудно перечислить математиков, участвовавших в построении теории разбиений натуральных чисел в сумму натуральных слагаемых после того, как Эйлер доказал о них первые теоремы. Большинство исследований были направлены на вычисление чисел разбиений различных видов и вывод алгебраических и комбинаторных соотношений между классами разбиений. В последние десятилетия усилился интерес к разбиениям чисел со стороны физиков [10], хотя асимптотическую формулу Харди–Рамануджана для числа разбиений впервые применили в ядерной физике уже Бор и Калкар [9]. В [12] предложен новый подход к изучению разбиений чисел, при котором каждое разбиение числа n отождествляется с точкой $\mathbb{R}^n$, а множество всех разбиений n рассматривается как политоп (ограниченный выпуклый многогранник) $P_n \subset \mathbb{R}^n$. Полиэдральный подход дал возможность исследовать комбинаторно-геометрическую структуру множества разбиений.

Исходной для данной работы послужила задача распознавания вершин политопа P_n среди всех разбиений числа n. Мы исследуем вычислительную сложность варианта этой задачи — распознавания разбиений, не представимых в виде выпуклой комбинации двух разбиений того же числа. Класс таких разбиений совпадает с классом рюкзачных разбиений [11] и с классом введенных нами мультимножеств Сидона, который включает в себя известные структуры аддитивной комбинаторики: множества без сумм, стандартные и обобщенные множества Сидона [14]. Доказано, что задача распознавания рюкзачных разбиений со-NP-полна и, следовательно, неразрешима за полиномиальное время, если верна гипотеза $P \neq NP$.

Политоп разбиений P_n есть частный случай политопа на частичной алгебре [4], который является обобщением многогранника на группе, возникающего при применении теоретико-группового подхода к задаче целочисленного линейного программирования [3]. В [12] описаны все фасеты (грани максимальной размерности) политопов P_n в виде определенных решений системы уравнений и неравенств. Объектом дальнейших исследований стали вершины P_n, поскольку они впервые дают возможность свести все множество разбиений числа n к подмножеству: каждое разбиение n является выпуклой комбинацией вершин. Таким образом, вершины P_n образуют своеобразный базис множества всех разбиений n.

Первые раздельные достаточные и необходимые условия для того, чтобы разбиение являлось вершиной политопа разбиений, получены в [12]. В [5] доказан критерий представления разбиения в виде выпуклой комбинации двух разбиений: такое представление возможно тогда и только тогда, когда существуют два различных набора входящих в заданное разбиение слагаемых, имеющие равные суммы. Из критерия последовали новые необходимые условия для вершин, в частности точная верхняя оценка числа различных слагаемых в разбиениях-вершинах.

В [6, 12] введены две комбинаторные операции на разбиениях и показано, что их применение к вершинам P_n приводит к его вершинам. Таким образом, оказалось, что все вершины политопа разбиений можно построить с помощью двух операций из существенно меньшего числа вершин, названных опорными, — тех, которые невозможно получить из других вершин, используя эти операции. Это означает, что вершинный базис множества разбиений можно существенно уменьшить, ограничившись опорными вершинами политопа.

В [5] предложен метод лифтинга для построения вершин всех политопов разбиений. При его выполнении множество тех разбиений n, среди которых ищутся вершины P_n, существенно сужается: все вершины индуцируются определенными разбиениями некоторых чисел меньших n. Проверка, являются ли полученные разбиения вершинами P_n, оказалась непростой задачей.

Рассматриваемый в работе вариант задачи распознавания вершин политопа P_n выглядит наиболее простым, поскольку для многих чисел $n \geqslant 15$ существуют разбиения, требующие более двух других для своего выпуклого представления [7], и, следовательно, установленный критерий характеризует не все вершины P_n. Однако мы показываем, что именно в этом варианте рассматриваемая задача полиномиально неразрешима при условии $P \neq NP$. При этом существование полиномиального алгоритма решения общей задачи распознавания вершин политопов разбиений остается возможным, но мы не отказываемся от высказанной в [7] гипотезы, что эта задача NP-трудна. Доказанная co-NP-полнота задач распознавания рюкзачных разбиений и мультимножеств Сидона представляет, на наш взгляд, самостоятельный интерес.

Для доказательства co-NP-полноты основной задачи мы устанавливаем NP-полноту задачи распознавания разбиений, *представимых* в виде выпуклой комбинации *двух* других разбиений того же числа, сводя к ней одну из шести основных NP-полных задач — комбинаторную задачу Разбиение [1]. При этом существенно используется критерий [5].

1. ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ И РАССМАТРИВАЕМЫЕ ЗАДАЧИ

Разбиением натурального числа n называется конечная невозрастающая последовательность натуральных чисел $\rho = (\rho_1, \rho_2, \ldots, \rho_r)$, для которых

$\sum\limits_{j=1}^{r} \rho_j = n$ [8]. Числа $\rho_1, \rho_2, \ldots, \rho_r$ называют частями разбиения ρ. Каждому разбиению ρ числа n мы сопоставляем неотрицательную целочисленную точку $x = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$. Координата x_i точки x равна числу вхождений числа i в разбиение ρ, $i = 1, \ldots, n$, т. е. x является решением уравнения $x_1 + 2x_2 + \ldots + nx_n = n$ в неотрицательных целых числах. В дальнейшем мы отождествляем разбиения ρ с соответствующими им точками x. То, что точка x является разбиением числа n, мы обозначаем $x \vdash n$. Множество всех различных частей разбиения $x \vdash n$ обозначаем через S_x, $S_x = \{i \in \{1, \ldots, n\} \,|x_i > 0\}$, через $\mathbb{Z}_+$ — множество неотрицательных целых чисел и через $[n_1, n_2]$ — отрезок натуральных чисел $\{n_1, n_1+1, \ldots, n_2\}$.

Политоп разбиений числа n определяется как выпуклая оболочка множества всех разбиений n [12]:

$$P_n = \mathrm{conv.hull}\{x \in \mathbb{R}^n_+ | x \vdash n\}.$$

Напомним, что для произвольного политопа $P \subset \mathbb{R}^n$ точка $x \in P$ не является вершиной P тогда и только тогда, когда существует ее представление в виде выпуклой комбинации некоторых k, $2 \leqslant k \leqslant n+1$, точек политопа P, см., например, [2]. В частности, разбиение $x \vdash n$ не является вершиной P_n, если x представимо в виде выпуклой комбинации двух разбиений $y, z \vdash n$:

$$x = \lambda y + (1-\lambda) z, \text{ где } 0 < \lambda < 1. \tag{1}$$

Следующая теорема описывает разбиения, представимые в виде (1).

Теорема А [5]. Разбиение $x = (x_1, \ldots, x_n) \vdash n$ является выпуклой комбинацией двух разбиений числа n тогда и только тогда, когда существуют два непересекающихся подмножества частей разбиения x, $S_1, S_2 \subset S_x$, и два целочисленных набора $u = \langle u_s \in \mathbb{Z}_+;\ s \in S_1 \rangle$ и $v = \langle v_s \in \mathbb{Z}_+;\ s \in S_2 \rangle$, удовлетворяющие соотношениям

$$\sum_{s \in S_1} u_s s = \sum_{s \in S_2} v_s s, \quad 0 < u_s \leqslant x_s, \quad 0 < v_s \leqslant x_s. \tag{2}$$

Основная рассматриваемая в работе задача распознавания следующая.

Разбиение, непредставимое в виде выпуклой комбинации двух разбиений. Для заданного разбиения $x = (x_1, \ldots, x_n) \vdash n$ определить, верно ли, что не существует двух разбиений $y, z \vdash n$ и числа λ, удовлетворяющих условиям (1).

Понятно, что вершины политопов разбиений чисел находятся среди тех разбиений, для которых эта задача имеет ответ «да». Введенные в [11] рюкзачные разбиения — это те, все наборы частей которых дают различные суммы. По теореме А класс рюкзачных разбиений совпадает с классом разбиений, непредставимых в виде выпуклой комбинации двух других. Следовательно, класс вершин всех политопов разбиений чисел является собственным подклассом класса рюкзачных разбиений. Таким образом, основную задачу можно переформулировать в следующем виде.

Рюкзачное разбиение. Является ли заданное разбиение $x = (x_1, \dots, x_n) \vdash n$ рюкзачным?

В дальнейшем для краткости мы будем использовать эту постановку. Через $\text{size}(Z)$ обозначим размер задачи распознавания Z, равный длине двоичной записи ее входа. Равенство $f(t) = \mathcal{O}(g(t))$, где $f(k)$ и $g(k)$ — некоторые числовые функции, обозначает, что $f(t) \leqslant cg(t)$ для всех $k \geqslant 0$ при некоторой константе c. Через $p(k)$ обозначаем некоторую полиномиальную функцию на $\mathbb{N}$.

Входом задачи *Рюкзачное разбиение* является набор из n чисел $x_i \in \mathbb{Z}_+$, $x_i \leqslant n$, $i = 1, \dots, n$, поэтому ее размер равен $\mathcal{O}(n \log n)$.

Рюкзачные разбиения напоминают известные в комбинаторной теории чисел множества без сумм (sum-free sets) и множества Сидона [14]. Множествами Сидона (или B_2-множествами) называют такие множества $A \subset \mathbb{N}$, для которых $a_1 + a_2 \neq a_3 + a_4$ для всех $a_1, a_2, a_3, a_4 \in A$. В определении обобщенных множеств Сидона порядка $h > 2$ (или B_h-множеств) вместо пар элементов в левой и правой суммах фигурируют любые наборы по h элементов из A. В случае множеств без сумм запрещаются равенства $a_1 + a_2 = a_3$ для всех $a_1, a_2, a_3 \in A$.

Заметим, что в определениях множеств без сумм и множеств Сидона слагаемые разрешается повторять сколько угодно раз, в то время как в случае рюкзачных разбиений число повторений каждой части $s \in [1, n]$ разбиения числа n не превосходит x_s. Тем не менее все перечисленные структуры можно объединить как частные случаи определенных мультимножеств.

Под мультимножеством $\mathbb{A} = \langle A, m \rangle$ понимается пара, состоящая из множества A и неотрицательной целочисленнозначной функции кратности $m : A \to \mathbb{N}$. Всюду в дальнейшем рассматриваются только конечные мультимножества натуральных чисел. Мультимножество $\mathbb{B} = \langle B, m_B \rangle$ есть подмультимножество мультимножества $\mathbb{A}$ (обозначается $\mathbb{B} \subseteq \mathbb{A}$), если $B \subseteq A$ и $m_B(b) \leqslant m(b)$ для всех $b \in B$. Мультимножества $\mathbb{B} = \langle B, m_B \rangle$ и $\mathbb{C} = \langle C, m_C \rangle$ считаются непересекающимися ($\mathbb{B} \cap \mathbb{C} = \varnothing$), если $B \cap C = \varnothing$. Для $\mathbb{B} \subseteq \mathbb{A}$ через m'_B обозначается продолжение его функции кратности m_B на все множество A нулевыми значениями: $m'_B(a) = 0$ для $a \in A \backslash B$. Мультимножество $\mathbb{C} = \langle C, m_C \rangle$ назовем дополнением подмультимножества $\mathbb{B} \subseteq \mathbb{A}$ (обозначаем $\mathbb{C} = \mathbb{A} \backslash \mathbb{B}$), если $B \cup C = A$ и $m'_C(a) = m(a) - m'_B(a)$ для всех $a \in A$.

Каждое разбиение $x \vdash n$ можно рассматривать как мультимножество $\mathbb{S}_x = \langle S_x, m_x \rangle$ такое, что его функция кратности m_x имеет значения $m_x(s) = x_s$ для всех $s \in S_x$ и $\sum\limits_{s \in S_x} m_x(s)s = n$. Верно и обратное: каждое мультимножество (натуральных чисел) $\mathbb{A} = \langle A, m \rangle$ определяет разбиение x числа

$n = \sum\limits_{a \in A} m(a)a$. Необходимо взять $S_x = A$ и построить точку x с координатами $x_a = m(a)$ для $a \in S_x$ и $x_a = 0$ для $a \in [1, n] \backslash S_x$.

Теорему A легко выразить на языке мультимножеств. Подмножества $S_1, S_2 \subset S_x$ и наборы u, v определяют подмультимножества $\mathbb{S}_1 = \langle S_1, u \rangle$ и $\mathbb{S}_2 = \langle S_2, v \rangle$ мультимножества $\mathbb{S}_x$, а условие (2) принимает вид

$$\sum_{s \in S_1} m_{S_1}(s)s = \sum_{s \in S_2} m_{S_2}(s)s.$$

Определение. Мультимножество $\mathbb{A} = \langle A, m \rangle$, $A \subset \mathbb{N}$, назовем мультимножеством Сидона, если для любых двух его подмультимножеств $\mathbb{B} = \langle B, m_B \rangle$ и $\mathbb{C} = \langle C, m_C \rangle$ равенство

$$\sum_{a \in B} m_B(a)a = \sum_{a \in C} m_C(a)a \tag{3}$$

возможно только при равенстве подмультимножеств $\mathbb{B}$ и $\mathbb{C}$.

Иными словами, в мультимножестве Сидона все подмультимножества имеют различные суммарные веса своих элементов. Нетрудно видеть, что рюкзачным разбиениям $x \vdash n$ однозначно соответствуют мультимножества Сидона $\mathbb{S}_x = \langle S_x, m_x \rangle$ и наоборот.

В мультимножествах Сидона число повторений каждого слагаемого $s \in [1, n]$ в суммах (3) также ограничено кратностью x_s данного элемента s. Однако, взяв мультимножество Сидона $\langle A, m \rangle$ с $m(a) \geqslant 2h$ для всех $a \in A$ и добавив к (3) условия $\sum\limits_{a \in B} m_B(a) = \sum\limits_{a \in C} m_C(a) = h$, мы получим B_h-множество A, а в случае $h = 2$ — обычное множество Сидона. Наложив условия $m(a) \geqslant 3$, $\sum\limits_{a \in B} m_B(a) = 2$, $\sum\limits_{a \in C} m_C(a) = 1$, получим, что множество A является множеством без сумм. Таким образом, мультимножества Сидона обобщают рассмотренные выше аддитивные структуры и их введение вполне естественно. Так же естественно возникает и задача их распознавания.

Мультимножество Сидона. Для заданного мультимножества $\mathbb{A} = \langle A, m \rangle$ определить, является ли оно мультимножеством Сидона.

Эта задача и задача распознавания рюкзачных разбиений имеют на входе различные объекты: мультимножество и точку. Однако следующая лемма показывает, что размер разбиения $x \vdash n$, рассматриваемого как точка $\mathbb{R}^n$, полиномиально эквивалентен размеру этого разбиения, рассматриваемого как мультимножество $\mathbb{S}_x = \langle S_x, m_x \rangle$.

Лемма 1. Размер мультимножества $\mathbb{A} = \langle A, m \rangle$ равен $\mathcal{O}(n)$, где $n = \sum\limits_{a \in A} m(a)a$.

Доказательство. Мультимножество $\mathbb{A}$ задается двумя последовательностями натуральных чисел $(a,\ a \in A)$ и $(m(a),\ a \in A)$ длины $q = |A| < n$.

Их размер $\sum\limits_{a\in A}\log a+\sum\limits_{a\in A}\log m(a)=\log\prod\limits_{a\in A}m(a)a$ принимает максимальное значение, когда достигает максимума произведение. Из неравенства Коши о среднем арифметическом и среднем геометрическом получаем $\prod\limits_{a\in A}m(a)a\leqslant\left(\dfrac{\sum\limits_{a\in A}m(a)a}{q}\right)^q=\left(\dfrac{n}{q}\right)^q$. Исследуя функцию $y(x)=\left(\dfrac{n}{x}\right)^x$ на максимум на интервале $1\leqslant x<n$, получаем, что производная $y'=\left(\dfrac{n}{x}\right)^x\left(\ln\dfrac{n}{x}-1\right)=0$ при $x=\dfrac{n}{e}$. Так как $y''\left(\dfrac{n}{e}\right)<0$, то $x=\dfrac{n}{e}$ — точка максимума функции $\left(\dfrac{n}{x}\right)^x$, и $\max\limits_{1\leqslant q\leqslant n}\left(\dfrac{n}{q}\right)^q$ достигается при $q=\left[\dfrac{n}{e}\right]$ или $q=\left[\dfrac{n}{e}\right]+1$. В любом случае $\max\log\prod\limits_{a\in A}m(a)a\approx\log\left(\dfrac{n}{n/e}\right)^{n/e}=\dfrac{n}{e}=\mathcal{O}(n)$. Поскольку при $m(a_1)a_1=m(a_2)a_2=\ldots=m(a_q)a_q$ неравенство Коши обращается в равенство, полученный размер достижим. Лемма доказана.

2. ОСНОВНОЙ РЕЗУЛЬТАТ И ПРОМЕЖУТОЧНЫЕ ЗАДАЧИ

В работе доказана

Теорема. Задача *Рюкзачное разбиение* со-NP-полна.

Со-NP-полнота некоторой задачи распознавания означает, что дополнительная к ней задача NP-полна [1]. Дополнительной к задаче *Рюкзачное разбиение* является задача

Выпуклая комбинация двух разбиений чисел. Для заданного разбиения $x=(x_1,\ldots,x_n)\vdash n$ определить, верно ли, что существуют два разбиения $y,z\vdash n$ и число λ, удовлетворяющие (1).

Размер этой задачи по-прежнему равен $\mathcal{O}(n\log n)$. Ее NP-полноту мы доказываем, сводя к ней комбинаторную задачу *Разбиение*, одну из шести основных NP-полных задач [1].

Разбиение. Для заданного конечного множества T с весами $w(t)\in\mathbb{N}$ своих элементов определить, существует ли в нем такое подмножество $T_1\subset T$, что $\sum\limits_{t\in T_1}w(t)=\sum\limits_{t\in T\setminus T_1}w(t)$.

Вход задачи *Разбиение* состоит из $|T|$ весов $w(t)$, и ее размер равен $\mathcal{O}(|T|\log w_{\max})$, где $w_{\max}=\max\left(w(t),t\in T\right)$.

В процессе сведения рассматриваются еще несколько задач распознавания и устанавливается их NP-полнота.

Непересекающиеся подмультимножества равного веса. Для заданного мультимножества $\mathbb{A} = \langle A, m \rangle$ определить, существуют ли в нем два непересекающихся подмультимножества $\mathbb{B} = \langle B, m_B \rangle$ и $\mathbb{C} = \langle C, m_C \rangle$, удовлетворяющие равенству (3).

Неравные подмультимножества равного веса. Для заданного конечного мультимножества $\mathbb{A} = \langle A, m \rangle$ определить, существуют ли в нем два различных подмультимножества $\mathbb{B} = \langle B, m_B \rangle$ и $\mathbb{C} = \langle C, m_C \rangle$, удовлетворяющие (3).

Разбиение мультимножества. Для заданного мультимножества $\mathbb{A} = \langle A, m \rangle$ определить, существует ли в нем подмультимножество $\mathbb{B} = \langle B, m_B \rangle$ такое, что $\mathbb{B}$ и $\mathbb{C} = \langle C, m_C \rangle = \mathbb{A} \backslash \mathbb{B}$ удовлетворяют (3).

В доказательстве теоремы используются три леммы.

Лемма 2. Задача *Разбиение* полиномиально сводится к задаче *Разбиение мультимножества*.

Лемма 3. Задача *Неравные подмультимножества равного веса* полиномиально сводится к задаче *Непересекающиеся подмультимножества равного веса*.

Лемма 4. Задача *Непересекающиеся подмультимножества равного веса* полиномиально сводится к задаче *Выпуклая комбинация двух разбиений чисел*.

3. ДОКАЗАТЕЛЬСТВО ОСНОВНОЙ ТЕОРЕМЫ

Поскольку класс co-NP-полных задач совпадает с классом задач, дополнительных к NP-полным [1], для доказательства теоремы нужно показать, что задача *Выпуклая комбинация двух разбиений чисел* NP-полна.

Покажем, что эта задача принадлежит классу NP. Пусть Z — некоторая ее индивидуальная задача с разбиением $x \vdash n$ на входе. Ее размер равен $\text{size}(Z) = \mathcal{O}(n \log n)$. Нужно показать, что размер «угаданных» разбиений $y, z \vdash n$, выпуклой комбинацией (1) которых является разбиение x, ограничен полиномом от размера Z и что проверка того, что разбиения y и z действительно дают решение задачи, осуществима за время $\mathcal{O}(p(\text{size}(Z)))$. Разбиения $y, z \vdash n$ рассматриваются как точки $\mathbb{R}^n$, поэтому их совокупный размер равен $\mathcal{O}(n \log n)$.

То, что y и z — разбиения n, легко проверить за полиномиальное от $\text{size}(Z)$ время, вычислив суммы $\sum\limits_{i=1}^{n} y_i i$ и $\sum\limits_{i=1}^{n} z_i i$. Проверку представления (1) разбиения x можно выполнить за время $\mathcal{O}(p(n))$: достаточно убедиться в том, что λ удовлетворяет равенствам $x_i = \lambda y_i + (1-\lambda) z_i$, $i = 1, \ldots, n$, и условиям $0 < \lambda < 1$.

Теперь докажем, что NP-полная задача *Разбиение* полиномиально сводится к задаче *Выпуклая комбинация двух разбиений чисел*. При этом мы будем говорить, что промежуточные задачи NP-полны, опуская доказательства их принадлежности классу NP. Это нетрудно доказать непосредственно, но в конечном счете эти утверждения следуют из только что доказанной принадлежности NP задачи *Выпуклая комбинация двух разбиений чисел*.

Из леммы 2 получаем, что задача *Разбиение* полиномиально сводится к задаче *Разбиение мультимножества* и, значит, с учетом сделанного соглашения, последняя задача NP-полна. Она останется NP-полной и после добавления условия $\mathbb{B} \neq \mathbb{A} \backslash \mathbb{B} = \mathbb{C}$, поскольку существование разбиения мультимножества $\mathbb{A} = \langle A, x \rangle$ на равные $\mathbb{B}$ и $\mathbb{C}$, очевидно, проверяется за полиномиальное от размера $\mathbb{A}$ время, — достаточно проверить четность всех $x(a)$, $a \in A$. Задача *Разбиение мультимножества* с условием $\mathbb{B} \neq \mathbb{A} \backslash \mathbb{B} = \mathbb{C}$ является частным случаем задачи *Неравные подмультимножества равного веса*: к последней задаче нужно добавить условие $\mathbb{C} = \mathbb{A} \backslash \mathbb{B}$. Следовательно, и эта задача NP-полна. Теперь по лемме 3 NP-полной является задача *Непересекающиеся подмультимножества равного веса*. Применив лемму 4, заключаем, что NP-полна задача *Выпуклая комбинация двух разбиений чисел*. Теорема доказана.

Следствие 1. Задачи распознавания *Разбиение мультимножества*, *Неравные подмультимножества равного веса* и *Непересекающиеся подмультимножества равного веса* NP-полны.

Согласно теории сложности [1], из теоремы непосредственно вытекает

Следствие 2. Задачи распознавания *Рюкзачное разбиение* и *Мультимножество Сидона* co-NP-полны и, следовательно, если верна гипотеза $P \neq NP$, неразрешимы за полиномиальное время.

4. ДОКАЗАТЕЛЬСТВА ЛЕММ

Доказательство леммы 2. Пусть Z_1 — индивидуальная задача *Разбиение* на множестве T с весами элементов $w(t) \in \mathbb{N}$, $t \in T$. Ее размер равен $\mathcal{O}(|T| \log w_{\max})$. Построим множество A всех различных весов элементов из T. Для каждого $a \in A$ определим $T_a = \{t \in T | w(t) = a\}$ и $m(a) = |T_a|$. Получим мультимножество $\mathbb{A} = \langle A, m \rangle$, на котором рассмотрим индивидуальную задачу Z_2 задачи *Разбиение мультимножества*. Нетрудно показать, что размер $\mathrm{size}(Z_2)$ ограничен полиномом от $\mathrm{size}(Z_1)$ и что задачи Z_1 и Z_2 имеют ответ «да» одновременно. Если $T_1 \subset T$ доставляет ответ «да» в задаче Z_1, то подмультимножество $\mathbb{B} = \langle B, m_B \rangle \subset \mathbb{A}$, где $B = \{a \in A | |T_1 \cap T_a| > 0\}$ и $m_B(a) = |T_1 \cap T_a|$ для всех $a \in A$, доставляет ответ «да» в задаче Z_2. Обратно, пусть $\mathbb{B} = \langle B, m_B \rangle \subset \mathbb{A}$ доставляет ответ «да» в задаче Z_2 и $\mathbb{C} = \langle C, m_C \rangle = \mathbb{A} \backslash \mathbb{B}$. Тогда $m'_C(a) = m(a) - m'_B(a)$, $a \in A$. Включим в $T_1 \subset T$ по $m'_B(a)$ элементов из подмножеств T_a, $a \in A$. Нетрудно проверить, что $\sum\limits_{t \in T_1} w(t) = \sum\limits_{t \in T \backslash T_1} w(t)$, откуда следует, что T_1 доставляет ответ «да» в задаче Z_1. Лемма доказана.

Доказательство леммы 3. Так как обе задачи имеют на входе мультимножество $\mathbb{A} = \langle A, x \rangle$, достаточно показать, что они одновременно имеют положительный ответ.

Поскольку из $\mathbb{B} \cap \mathbb{C} = \varnothing$ следует $\mathbb{B} \neq \mathbb{C}$, ответ «да» во второй задаче влечет ответ «да» в первой задаче. Обратно, пусть подмультимножества $\mathbb{B} = \langle B, m_B \rangle \subset \mathbb{A}$, $\mathbb{C} = \langle C, m_C \rangle \subset \mathbb{A}$, $\mathbb{B} \neq \mathbb{C}$, доставляют ответ «да» в первой задаче. Если $\mathbb{B} \cap \mathbb{C} = \varnothing$, то $\mathbb{B}$ и $\mathbb{C}$ доставляют положительный ответ и во второй задаче. В случае $\mathbb{B} \cap \mathbb{C} \neq \varnothing$ построим непустые подмультимножества $\mathbb{B}^* = \langle B^*, m_B^* \rangle$ и $\mathbb{C}^* = \langle C^*, m_C^* \rangle$ мультимножества $\mathbb{A}$, удовлетворяющие условиям $\mathbb{B}^* \cap \mathbb{C}^* = \varnothing$ и

$$\sum_{a \in B^*} m_B^*(a)a = \sum_{a \in C^*} m_C^*(a)a. \tag{4}$$

Определим $B^* = \{a \in B | m'_B(a) > m'_C(a)\}$ и $C^* = \{a \in B | m'_B(a) < m'_C(a)\}$. Функции $m_B^* : B^* \to \mathbb{N}$ и $m_C^* : C^* \to \mathbb{N}$ определим как ограничения функций $m_B(a) - \min(m'_B(a), m'_C(a))$ и $m_C(a) - \min(m'_B(a), m'_C(a))$ на B^* и C^* соответственно. Легко видеть, что $\mathbb{B}^*, \mathbb{C}^* \neq \varnothing$ и $\mathbb{B}^* \cap \mathbb{C}^* = \varnothing$. Справедливость (4) также нетрудно проверить: она объясняется тем, что мы удалили из (3) совпадающие слагаемые. Лемма доказана.

Доказательство леммы 4. Пусть Z_1 — индивидуальная задача *Непересекающиеся подмультимножества равного веса* с мультимножеством $\mathbb{A} = \langle A, m \rangle$ на входе. $\mathbb{A}$ определяет разбиение $x \in \mathbb{R}^n_+$ числа $n = \sum\limits_{a \in A} m(a)a$, заданное в форме $\mathbb{S}_x = \langle S_x, m_x \rangle$, где $S_x = A$, $m_x = m$. По лемме 1 точку x можно построить за полиномиальное от $\mathrm{size}(Z_1)$ время. Для $x \vdash n$ рассмотрим индивидуальную задачу Z_2 задачи *Выпуклая комбинация двух разбиений чисел*. По теореме А задачи Z_1 и Z_2 имеют ответ «да» одновременно, поскольку непересекающиеся подмножества $S_1, S_2 \subset S_x$ и наборы $u = \langle u(a) \in \mathbb{N};\ a \in S_1 \rangle$ и $v = \langle v(a) \in \mathbb{N};\ a \in S_2 \rangle$, удовлетворяющие (2), определяют непересекающиеся подмультимножества $\mathbb{B} = \langle S_1, m_{S_1} = u \rangle$ и $\mathbb{C} = \langle S_2, m_{S_2} = v \rangle$ в $\mathbb{A}$ и наоборот. Условия (3) для мультимножеств и (2) для S_1, S_2, u, v эквивалентны друг другу. Лемма доказана.

Благодарности. Автор признателен Е. А. Барабанову, В. М. Демиденко, М. Я. Ковалеву и С. И. Тарасову за полезные обсуждения и советы.

ЛИТЕРАТУРА

1. *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.
2. *Рокафеллар Р.* Выпуклый анализ. М.: Мир, 1973.
3. *Ху Т.* Целочисленное программирование и потоки в сетях. М.: Мир, 1974.

4. *Шлык В. А.* Субаддитивная характеризация граней многогранных множеств на частичной алгебре // Доклады Академии наук БССР. 1984. Т. 28, № 2. С. 980–983.
5. *Шлык В. А.* О вершинах политопов разбиений чисел // Доклады НАН Беларуси. 2008. Т. 52, № 3. С. 5–10.
6. *Шлык В. А.* Комбинаторные операции порождения вершин политопа разбиений чисел // Докл. НАН Беларуси. 2009. Т. 53, № 6. С. 27–32.
7. *Шлык В. А.* Критерий представления разбиений чисел в виде выпуклой комбинации двух разбиений // Вестник БГУ. Сер. 1. 2009. № 2. С. 109–114.
8. *Эндрюс Г.* Теория разбиений. М.: Наука, 1982.
9. *Bohr N., Kalckar F.* On the Transmutation of Atomic Nuclei by Impact of Material Particles: I. General theoretical remarks // Kgl. Danske Vid. Selsk. Skr. 1937. V. 14. P. 1–40.
10. *Debnath L.* Srinivasa Ramanujan (1887–1920) and the Theory of Partitions of Numbers and Statistical Mechanics. A Centennial Tribute // Intern. J. Math. and Math. Sci. 1987. V. 10, No. 4. P. 625–640.
11. *Ehrenborg R., Readdy M. A.* The Möbius Function of Partitions with Restricted Block Sizes // Advances in Applied Mathematics. 2007. V. 39, No. 3. P. 283–292.
12. *Shlyk V. A.* Polytopes of Partitions of Numbers // European J. Combinatorics. 2005. V. 26, No. 8. P. 1139–1153.
13. *Shlyk V. A.* Recursive Operations for Generating Vertices of Integer Partition Polytopes. JINR Communication E5-2008-18. Dubna, 2008.
14. *Tao T., Vu V. H.* Additive Combinatorics. Cambridge: Cambridge University Press, 2006.

Получено 31 марта 2010 г.

Редактор *А. И. Петровская*

Подписано в печать 26.05.2010.
Формат $60 \times 90/16$. Бумага офсетная. Печать офсетная.
Усл. печ. л. 0,81. Уч.-изд. л. 0,95. Тираж 315 экз. Заказ № 57006.

Издательский отдел Объединенного института ядерных исследований
141980, г. Дубна, Московская обл., ул. Жолио-Кюри, 6.
E-mail: publish@jinr.ru
www.jinr.ru/publish/