Записки научных
семинаров ПОМИ
Том 378, 2010 г.

В. А. Шлык

ЗАДАЧИ РАСПОЗНАВАНИЯ НЕКОТОРЫХ КЛАССОВ РАЗБИЕНИЙ ЧИСЕЛ И ЧИСЛОВЫХ МУЛЬТИМНОЖЕСТВ

§1. Введение

Разбиение натурального числа в сумму натуральных слагаемых – одно из фундаментальных математических понятий. Разбиения чисел связаны с различными направлениями алгебры, теории чисел, комбинаторного анализа, теории представлений и др., см. [3, 7]. Трудно перечислить математиков, участвовавших в построении теории разбиений 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 (см. [9]), поскольку они находят применения в статистической механике, ядерной и квантовой физике. Впервые связь асимптотической формулы Харди–Рамануджана для числа разбиений с одной из задач ядерной физики отметили Бор и Калкар [8].

При исследовании разбиений чисел обычно применяют аппарат производящих функций и технику таблиц Юнга (см. [3]), основанную на их двумерном геометрическом представлении. В [11] предложен новый подход к изучению разбиений чисел, при котором каждое разбиение числа n отождествляется с точкой пространства $\mathbb{R}^n$, а множество всех таких разбиений рассматривается как политоп (ограниченный выпуклый многогранник) $P_n \subset \mathbb{R}^n$. Полиэдральный подход впервые дал возможность исследовать пространственную комбинаторно-геометрическую структуру множества разбиений каждого числа и свести его к собственному подмножеству.

Исходной для данной работы послужила задача распознавания вершин политопа P_n среди всех разбиений числа n. Мы исследуем вычи-

---

Ключевые слова: политопы разбиений чисел, вершины политопов, мультимножества Сидона, задачи распознавания, NP-полнота.

слительную сложность варианта этой задачи: распознавания разбиений, не представимых в виде выпуклой комбинации двух разбиений того же числа. Мы доказываем, что класс таких разбиений совпадает с классом рюкзачных разбиений (см. [10]) и с классом введенных нами мультимножеств Сидона. Последний близок к таким известным структурам аддитивной комбинаторики, как множества без сумм, стандартные и обобщенные множества Сидона (см. [13]). В работе доказано, что задачи распознавания указанных классов разбиений со-NP-полны и, следовательно, неразрешимы за полиномиальное время, если верна гипотеза $P \neq NP$. Вместе с этим доказана NP-трудность задач распознавания рюкзачных разбиений и мультимножеств Сидона, что представляет самостоятельный интерес. Полученный результат не отвергает существование полиномиального алгоритма решения общей задачи распознавания вершин политопов разбиений, но мы не отказываемся от высказанной в [6] гипотезы, что и эта задача NP-трудна.

Любой политоп определяется своими вершинами или фасетами (гранями максимальной размерности). Фасеты политопов разбиений описаны в виде определенных решений системы субаддитивных неравенств и уравнений, см. [11]. Несмотря на ожидаемую сложность, задача распознавания вершин политопов разбиений представляет особый интерес, поскольку каждое разбиение числа n является выпуклой комбинацией вершин политопа P_n и, значит, эти вершины образуют своеобразный базис множества разбиений. Более того, вычисления показывают, что с ростом n число вершин становится существенно меньше числа разбиений, достигая 15% уже для n порядка 20.

После первых достаточных и, отдельно, необходимых условий для того, чтобы разбиение являлось вершиной политопа разбиений (см. [11]), в [4] 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 [5, 12] введены две комбинаторные операции на разбиениях и показано, что при их применении вершины политопа P_n переводятся в вершины. Таким образом, оказалось, что вершинный базис множества разбиений можно существенно уменьшить, ограничившись теми вершинами, которые невозможно получить из других вершин, используя эти операции, – мы назвали такие разбиения опорными.

В [4] предложен метод лифтинга для последовательного построения вершин всех политопов разбиений. При его применении множество тех разбиений n, среди которых ищутся вершины политопа P_n, существенно сужается – все вершины индуцируются определенными разбиениями некоторых чисел меньших n. Проверка, являются ли полученные разбиения вершинами политопа P_n, оказалась непростой задачей.

Рассматриваемый в работе вариант задачи распознавания вершин политопа P_n выглядит наиболее простым, поскольку для многих чисел $n \geq 15$ существуют разбиения, требующие более двух других для своего выпуклого представления (см. [6]) и, следовательно, установленный критерий характеризует не все вершины политопа P_n. Однако мы показываем, что именно в этом варианте рассматриваемая задача полиномиально трудна.

Для доказательства co-NP-полноты рассматриваемой 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*”, см. [1]. При этом существенно используется критерий из работы [5].

В параграфе 2 приведены определения политопа разбиений чисел, рюкзачных разбиений и мультимножеств Сидона, критерий представления разбиения в виде выпуклой комбинации двух разбиений и три варианта рассматриваемой задачи. В третьем параграфе сформулированы основной результат работы, промежуточные задачи и вспомогательные леммы. Доказательство основной теоремы изложено в параграфе 4. В последнем параграфе приведены доказательства лемм и, для полноты изложения, упомянутого критерия.

§2. Предварительные сведения и рассматриваемые задачи

Разбиением натурального числа n называется такая конечная невозрастающая последовательность натуральных чисел $\rho = (\rho_1, \rho_2, \dots, \rho_r)$, для которой $\sum_{j=1}^{r} \rho_j = n$, см. [7]. Числа $\rho_1, \rho_2, \dots, \rho_r$ называют частями разбиения ρ. Каждому разбиению ρ числа n мы сопоставляем неотрицательную целочисленную точку $x = (x_1, x_2, \dots, x_n) \in \mathbb{R}^n$. Координата x_i точки x равна числу вхождений числа i в разбиение ρ, $i = 1, \dots, n$, 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. Запись $x \vdash n$ означает, что точка x является разбиением числа n. Через S_x обозначается множество всех различных частей разбиения $x \vdash n$, т.е. $S_x = \{i \in \{1, \dots, n\} \mid x_i > 0\}$, через $\mathbb{Z}_+$ – множество неотрицательных целых чисел и через $[n_1, n_2]$ – отрезок натуральных чисел $\{n_1, n_1 + 1, \dots, n_2\}$.

Политоп разбиений числа n определяется как выпуклая оболочка множества всех разбиений n (см. [11]):

$$P_n = \operatorname{conv}\{x \in \mathbb{R}^n_+ \mid x \vdash n\}.$$

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

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

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

Теорема 1 ([4]). *Разбиение $x = (x_1, x_2, \dots, x_n) \vdash n$ является выпуклой комбинацией двух разбиений числа n тогда и только тогда, когда существуют два непересекающихся подмножества $S_1, S_2 \subset S_x$ частей разбиения 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*

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

Основная рассматриваемая в работе задача распознавания такова.

Разбиение, непредставимое в виде выпуклой комбинации двух разбиений. Для заданного разбиения $x = (x_1, x_2, \dots, x_n) \vdash n$ определить, верно ли, что не существует двух разбиений $y, z \vdash n$ и числа λ, удовлетворяющих условиям (1).

Понятно, что для вершин политопов разбиений чисел эта задача имеет положительный ответ. Введенные в [10] рюкзачные разбиения

– это разбиения, все наборы частей которых дают различные суммы. По теореме 1 класс рюкзачных разбиений совпадает с классом разбиений, непредставимых в виде выпуклой комбинации двух других. Отсюда получаем, что 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 разбиение $x=(x_1,x_2,\ldots,x_n)\vdash n$ рюкзачным?

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

Входом задачи "*Рюкзачное разбиение*" является набор из n чисел $x_i\in\mathbb{Z}_+$, $x_i\le n$, $i=1,\ldots,n$, 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 (см. [13]). Множествами Сидона (или B_2-множествами) называют такие множества $A\subset\mathbb{N}$, для которых

$$a_1+a_2\ne a_3+a_4 \tag{3}$$

при любых $a_1,a_2,a_3,a_4\in A$, $\{a_1,a_2\}\ne\{a_3,a_4\}$. В определении обобщенных множеств Сидона порядка $h>2$ (или B_h-множеств) вместо пар элементов в левой и правой суммах равенства (3) 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 $x\vdash n$ не превосходит x_s. Тем не менее, все перечисленные структуры можно объединить, воспользовавшись мультимножествами.

Под мультимножеством $\mathbb{A}=\langle A,m\rangle$ понимается пара, состоящая из множества A и 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 $m_B(b) \leq m(b)$ 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 подмультимножества $\mathbb{B} \subseteq \mathbb{A}$ через m'_B обозначим продолжение его функции кратности m_B на все множество A нулевыми значениями: $m'_B(a) = 0$ для $a \in A \setminus B$. Мультимножество $\mathbb{C} = \langle C, m_C \rangle$ назовем дополнением подмультимножества $\mathbb{B} \subseteq \mathbb{A}$ (обозначаем $\mathbb{C} = \mathbb{A} \setminus \mathbb{B}$), 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 $\sum_{s \in S_x} m_x(s)s = n$. 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 $a \in [1, n] \setminus S_x$.

Теорему 1 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 1. *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*

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

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 a в суммах (4) также ограничено кратностью $m(a)$. Однако, взяв мультимножество Сидона $\mathbb{A} = \langle A, m \rangle$ с $m(a) \geq 2h$ для всех $a \in A$ и добавив к (4) 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 $m(a) \geq 2$, $\sum_{a\in B} m_B(a) = 2$, $\sum\limits_{a\in C} m_C(a) = 1$, мы получим множество без сумм. Таким образом, мультимножества Сидона, естественным образом возникшие при исследовании вершин политопов разбиений, родственны известным аддитивным структурам. Так же естественно возникает и задача их распознавания.

Мультимножество Сидона. Для 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 в $\mathbb{R}^n$, 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 $q = |A|$. Их размер $\sum\limits_{a\in A} \log a + \sum\limits_{a\in A} \log m(a)$ принимает максимальное значение, когда достигает максимума произведение $\prod\limits_{a\in A} m(a)a$. Из неравенства Коши о среднем арифметическом и среднем геометрическом получаем

$$\prod_{a\in A} m(a)a \leq \left(\frac{\sum\limits_{a\in A} m(a)a}{q}\right)^q = \left(\frac{n}{q}\right)^q.$$

Исследуя функцию $y(x) = \left(\frac{n}{x}\right)^x$ на максимум на интервале $1 \leq x < n$, получаем, что $y'(x) = \left(\frac{n}{x}\right)^x \left(\ln \frac{n}{x} - 1\right) = 0$ при $x = \frac{n}{e}$. Так как $y''\left(\frac{n}{e}\right) < 0$, мы видим, что $x = \frac{n}{e}$ – точка максимума функции $\left(\frac{n}{x}\right)^x$, и $\max\limits_{1\leq q\leq n} \left(\frac{n}{q}\right)^q$ достигается при $q = \left\lfloor \frac{n}{e} \right\rfloor$ или $q = \left\lfloor \frac{n}{e} \right\rfloor + 1$. В любом случае

$$\max \log \prod_{a\in A} m(a)a \approx \log\left(\frac{n}{n/e}\right)^{n/e} = \mathcal{O}(n).$$

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. □

§3. Основной результат и промежуточные задачи

В работе доказана следующая теорема.

Теорема 2. *Задача "Рюкзачное разбиение" co-NP-полна.*

co-NP-полнота некоторой задачи распознавания означает, что дополнительная к ней задача NP-полна, см. [1]. Дополнительной к задаче "*Рюкзачное разбиение*" является задача "*Выпуклая комбинация двух разбиений чисел*": для заданного разбиения $x = (x_1, x_2, \dots, x_n) \vdash n$ определить, существуют ли два разбиения $y, z \vdash n$ и число λ, удовлетворяющие условию (1).

NP-полноту этой задачи мы доказываем, сводя к ней следующую комбинаторную задачу

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

$$\sum_{t \in T_1} w(t) = \sum_{t \in T \setminus T_1} w(t).$$

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

В процессе сведения рассматриваются еще три задачи 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 (4).

Неравные подмультимножества равного веса. Для заданного 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 равенству (4).

Разбиение мультимножества. Для заданного мультимножества $\mathbb{A} = \langle A, m \rangle$ определить, существует ли в нем такое подмультимножество $\mathbb{B} = \langle B, m_B \rangle$, что $\mathbb{B}$ и $\mathbb{C} = \langle C, m_C \rangle = \mathbb{A} \setminus \mathbb{B}$ удовлетворяют равенству (4).

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".*

§4. Доказательство основной теоремы

Поскольку класс co-NP-полных задач совпадает с классом задач, дополнительных к NP-полным (см. [1]), для доказательства теоремы достаточно 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 $\mathrm{size}(Z) = \mathcal{O}(n \log n)$. Нужно показать, что размер "угаданных" разбиений $y, z \vdash n$, выпуклой комбинацией (1) которых является разбиение x, ограничен полиномом от $\mathrm{size}(Z)$ и что проверка того, что разбиения y и z действительно дают решение задачи, осуществима за время $\mathcal{O}(p(\mathrm{size}(Z)))$. Разбиения $y, z \vdash n$ рассматриваются как точки в $\mathbb{R}^n$, поэтому их совокупный размер равен $\mathcal{O}(n \log n)$. То, что y и z – разбиения числа n, легко проверить за полиномиальное от $\mathrm{size}(Z)$ время, вычислив суммы $\sum\limits_{i=1}^{n} y_i i$ и $\sum\limits_{i=1}^{n} z_i i$. Проверку представления (1) разбиения числа n можно выполнить за время $\mathcal{O}(p(n))$: достаточно убедиться в том, что λ удовлетворяет равенствам $x_i = \lambda y_i + (1-\lambda) z_i$, $i = 1, \dots, n$, 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. Эти утверждения нетрудно доказать непосредственно, но в конечном счете они следуют из только что доказанной принадлежности к классу NP задачи "*Выпуклая комбинация двух разбиений чисел*".

Из леммы 2 мы видим, что задача "*Разбиение*" полиномиально сводится к задаче "*Разбиение мультимножества*" и, значит, с учетом сделанного соглашения, последняя задача NP-полна. Она остается NP-полной и после добавления условия $\mathbb{B} \neq \mathbb{A} \setminus \mathbb{B} = \mathbb{C}$, 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 $\mathbb{B} \neq \mathbb{A} \setminus \mathbb{B} = \mathbb{C}$ является частным случаем задачи "*Неравные подмультимножества равного веса*": к последней задаче нужно добавить условие $\mathbb{C} = \mathbb{A} \setminus \mathbb{B}$. 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 (см. [1]), из теоремы непосредственно вытекает следствие.

Следствие 2. *Задачи распознавания "Разбиение, не представимое в виде выпуклой комбинации двух разбиений", "Рюкзачное разбиение" и "Мультимножество Сидона" co-NP-полны и, следовательно, если верна гипотеза $P \neq NP$, неразрешимы за полиномиальное время.*

§5. Доказательства лемм и теоремы 1

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 $a \in A$ положим $T_a = \{t \in T \mid w(t) = a\}$ и $m(a) = |T_a|$. Мы получим мультимножество $\mathbb{A} = \langle A, m \rangle$, на котором рассмотрим индивидуальную задачу Z_2 задачи "*Разбиение мультимножества*". Ее размер ограничен полиномом от $\operatorname{size}(Z_1)$, поскольку $|A| \leq |T|$, $a \leq w_{\max}$ для всех $a \in A$, а построение множества A, подмножеств T_a и вычисление $m(a)$, $a \in A$, осуществимо за время $\mathcal{O}(|T| \log w_{\max} + \log |T|)$.

Покажем, что задачи Z_1 и Z_2 имеют ответ "да" одновременно. Пусть подмножество $T_1 \subset T$ доставляет решение задачи Z_1 с ответом "да". Для каждого $a \in A$ обозначим $m'_B(a) = |T_1 \cap T_a|$. Положив $B = \{a \in A \mid m'_B(a) > 0\}$ и определив функцию $m_B : B \to \mathbb{N}$ как ограничение функции $m'_B : A \to \mathbb{N}$ на B, мы получим подмультимножество $\mathbb{B} = \langle B, m_B \rangle \subset \mathbb{A}$. Покажем, что $\mathbb{B}$ – решение задачи Z_2. Обозначим $\mathbb{C} = \langle C, m_C \rangle = \mathbb{A} \setminus \mathbb{B}$. Для каждого $a \in A$ в T_1 не попало

$m'_C(a) = m(a) - m'_B(a)$ элементов веса a, и, значит, $m_C : C \to \mathbb{N}$ есть ограничение на C функции $m'_C : A \to \mathbb{N}$. Имеет место равенство

$$\begin{aligned}\sum_{a\in B} m_B(a)a &= \sum_{a\in A} m'_B(a)a = \sum_{t\in T_1} w(t)\\ &= \sum_{t\in T\setminus T_1} w(t) = \sum_{a\in A}(m(a) - m'_B(a))a\\ &= \sum_{a\in A} m'_C(a)a = \sum_{a\in A} m_C(a)a.\end{aligned}$$

Обратно, пусть подмультимножество $\mathbb{B} = \langle B, m_B\rangle \subset \mathbb{A}$ доставляет ответ "да" в задаче Z_2. Обозначим $\mathbb{C} = \langle C, m_C\rangle = \mathbb{A} \setminus \mathbb{B}$. Включим в $T_1 \subset T$ по $m'_B(a)$ элементов из подмножеств T_a, $a \in A$. Тогда в $T \setminus T_1$ попадут по $m'_C(a) = m(a) - m'_B(a)$ элементов из T_a. Равенство

$$\begin{aligned}\sum_{t\in T_1} w(t) = \sum_{a\in A} m'_B(a)a = \sum_{a\in B} m_B(a)a = \sum_{a\in C} m_C(a)a =\\ = \sum_{a\in A} m'_C(a)a = \sum_{t\in T\setminus T_1} w(t)\end{aligned}$$

показывает, что T_1 доставляет ответ "да" в задаче Z_1. □

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

$$\sum_{a\in B^*} m^*_B(a)a = \sum_{a\in C^*} m^*_C(a)a. \tag{5}$$

Определим $B^* = \{a \in B \mid m'_B(a) > m'_C(a)\}$ и $C^* = \{a \in B \mid m'_B(a) < m'_C(a)\}$. 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. Нетрудно видеть, что $B^*, C^* \neq \varnothing$ и $B^* \cap C^* = \varnothing$. Справедливость равенства (5) также несложно проверить: она объясняется тем, что мы удалили из равенства (4) совпадающие слагаемые. □

Доказательство леммы 4. Пусть Z_1 – индивидуальная задача "*Непересекающиеся подмультимножества равного веса*" с мультимножеством $\mathbb{A} = \langle A, m \rangle$ на входе. Мультимножество $\mathbb{A}$ определяет разбиение $x \in \mathbb{Z}^n$ числа $n = \sum_{a \in A} m(a)a$, заданное в форме $\mathbb{S}_x = \langle S_x, m_x \rangle$, где $S_x = A$, $m_x = m$. Координаты точки x равны $x_i = m_x(i)$ для $i \in S_x$ и $x_i = 0$ для $i \in [1, n] \setminus S_x$, и ее можно построить за время $\mathcal{O}(n \log n)$ – полиномиальное от $\mathrm{size}(Z_1) = \mathcal{O}(n)$, см. лемму 1. Для $x \vdash n$ рассмотрим индивидуальную задачу Z_2 задачи "*Выпуклая комбинация двух разбиений чисел*". По теореме 1 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 соотношению (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 (4) для мультимножеств и (2) для S_1, S_2, u, v эквивалентны друг другу. □

Доказательство теоремы 1. Если известны подмножества S_1 и S_2 и наборы u и v, то разбиения $y, z \vdash n$, для которых x является полусуммой, можно построить, положив

$$\begin{aligned} &y_j = x_j + u_j,\ j \in S_1; \quad y_k = x_k - v_k,\ k \in S_2; \quad y_i = x_i,\ i \notin S_1 \cup S_2; \\ &z_j = x_j - u_j,\ j \in S_1; \quad z_k = x_k + v_k,\ k \in S_2; \quad z_i = x_i,\ i \notin S_1 \cup S_2. \end{aligned}$$

Обратно, пусть $x \vdash n$ есть выпуклая комбинация $x = z + \lambda(y - z)$, $0 < \lambda < 1$, двух разбиений $y, z \vdash n$. Тогда λ – рациональное число, $\lambda = \frac{p}{q}$, где p и q взаимно просты, q делит все компоненты вектора $y - z$, x есть полусумма разбиений $z + \frac{p-1}{q}(y - z)$ и $z + \frac{p+1}{q}(y - z)$ числа n и мы можем считать, что $x = \frac{1}{2}(y + z)$. Определим три подмножества частей разбиения x: $S = \{i \in S_x | x_i \neq y_i\}$, $S_1 = \{j \in S_x | x_j < y_j\}$ и $S_2 = \{k \in S_x | x_k > y_k\}$. Нетрудно видеть, что $S_1, S_2 \subset S_x$, $S_1 \cap S_2 = \varnothing$, $S_1 = \{j \in S_x | x_j > z_j\}$, $S_2 = \{k \in S_x | x_k < z_k\}$. Требуемые наборы u и v мы получим, положив $u_j = y_j - x_j$ для $j \in S_1$ и $v_k = x_k - y_k$ для $k \in S_2$. Из равенства $x = \frac{1}{2}(y + z)$ и неотрицательности компонент разбиений x, y, z заключаем, что $u_j < x_j$ и $v_k < x_k$, а из того, что $x, y \vdash n$, следует равенство (2). □

Литература

1. М. Гэри, Д. Джонсон, *Вычислительные машины и труднорешаемые задачи.* Мир, М. (1982).
2. Р. Рокафеллар, *Выпуклый анализ.* Мир, М. (1973).
3. У. Фултон, *Таблицы Юнга и их приложения к теории представлений и геометрии.* МЦНМО, М. (2006).
4. В. А. Шлык, *О вершинах политопов разбиений чисел.* — Доклады НАН Беларуси **52**, вып. 3 (2008), 5–10.
5. В. А. Шлык, *Комбинаторные операции порождения вершин политопа разбиений чисел.* — Доклады НАН Беларуси **53**, вып. 6 (2009), 27–32.
6. В. А. Шлык, *Критерий представления разбиений чисел в виде выпуклой комбинации двух разбиений.* — Вестн. БГУ, Сер. 1, вып. 2 (2009), 109–114.
7. Г. Эндрюс, *Теория разбиений.* Наука, М. (1982).
8. N. Bohr, F. Kalckar, *On the transmutation of atomic nuclei by impact of material particles: I. General theoretical remarks.* Kgl. Danske Vid. Selsk. Skr. **14** (1937), 1–40.
9. L. Debnath, *Srinivasa Ramanujan (1887-1920) and the theory of partitions of numbers and statistical mechanics. A centennial tribute.* — Internat. J. Math. Math. Sci. **10**, No. 4 (1987), 625–640.
10. R. Ehrenborg, M. A. Readdy, *The Möbius function of partitions with restricted block sizes.* — Adv. Appl. Math. **39**, No. 3 (2007), 283–292.
11. V. A. Shlyk, *Polytopes of partitions of numbers.* — European J. Combin. **26**, No. 8 (2005), 1139–1153.
12. V. A. Shlyk, *Recursive operations for generating vertices of integer partition polytopes.* — Communication of the Joint Institute for Nuclear Research E5-2008-18, Dubna (2008).
13. T. Tao, V. H. Vu, *Additive Combinatorics.* Cambridge Univ. Press, Cambridge (2006).

Shlyk V. A. 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 number 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, it cannot be solved in polynomial time unless P=NP.

Институт математики
Национальной Академии наук Беларуси,
ул. Сурганова, д. 11,
220072 Минск, Беларусь

E-mail: v.shlyk@gmail.com

Поступило 18 июля 2010 г.