Записки научных
семинаров ПОМИ
Том 448, 2016 г.

Ж. Э. Исомуродов, К. П. Кохась

НАБОР ИЗ 12 ЧИСЕЛ НЕ ВОССТАНАВЛИВАЕТСЯ ОДНОЗНАЧНО ПО СВОИМ 4-СУММАМ

1. Введение. Пусть дан произвольный набор из n вещественных чисел. Рассмотрим набор сумм всевозможных выборок по k чисел из этих n чисел, назовем такой набор *набором k-сумм*. При каких (n, k) можно однозначно восстановить исходный набор из n чисел, если нам известен набор k-сумм? Это вопрос из задачи Л. Мозера [7], опубликованной в *American Math. Monthly* в 1957 г. Задача оказалась нетривиальной, ей было посвящено несколько публикаций в 60-е [4, 8, 3] и 90-е [1, 2] годы прошлого века. В книге Р. Гая "Нерешенные проблемы теории чисел" эта задача приводится как одна из нерешенных задач аддитивной теории чисел [5, задача C5].

В 1958 г. Дж. Л. Селфридж и Э. Г. Штраус [8] доказали, что для случая $(n, 2)$ восстановление возможно только для n, не являющихся степенями двойки. В общем случае они описали систему диофантовых уравнений относительно переменных n и k; для пар (n, k), не удовлетворяющих этим уравнениям (это типичная ситуация), восстановление однозначно. Если же пара (n, k) удовлетворяет хотя бы одному из уравнений, как в случае $(12, 4)$, возможность восстановления неясна. В 1962 г. А. С. Френкель, Б. Гордон, Э. Г. Штраус [4] свели изучение этого вопроса к случаю наборов целых чисел и доказали, что при каждом k есть лишь конечное множество n, для которых исходный набор восстанавливается неоднозначно. Для "проблемных" случаев $(8, 2)$, $(16, 2)$, $(6, 3)$ и $(12, 4)$ они оценили сверху количество наборов из n чисел, которые могут иметь один и тот же набор k-сумм. В 1968 г. Дж. Ивелл [3] доказал что в случае $(6, 3)$ наибольшее число разных наборов, имеющих одинаковый набор k-сумм, равно четырем. В 1994 г. Д. В. Фомин и О. Т. Ижболдин [1] привели пример двух различных наборов, чьи наборы k-сумм совпадают, для случаев $(27, 3)$ и $(486, 3)$. Эта публикация оказалась не слишком известной на Западе, и в 1996 г. Я. Боман и С. Линуссон [2] привели аналогичные примеры.

Ключевые слова: аддитивная комбинаторика, наборы сумм.

Кроме упомянутого результата, Дж. Ивелл в работе [3] доказал с помощью достаточно громоздкого по тем временам счета, что в случае $(12,4)$ исходный набор восстанавливается однозначно. На самом деле это утверждение неверно, и ниже мы предъявляем ошибку, сделанную в [3]. При попытке "починить" доказательство Ивелла с помощью системы компьютерной алгебры Maple, мы построили пример двух наборов из 12 чисел, имеющих одинаковые наборы 4-сумм. Таким образом, верна следующая теорема.

Теорема 1. *В случае* $(12,4)$ *исходный набор не восстанавливается однозначно: существуют два набора целых чисел, имеющих одинаковые наборы* 4*-сумм.*

В [4] доказано, что не существует трех наборов, имеющих одинаковые наборы 4-сумм. Как показывают наши вычисления, пара наборов, имеющая совпадающие наборы 4-сумм, единственна (с точностью до сдвигов и растяжений).

2. Исходное доказательство. Пусть дан произвольный набор из n чисел
$$A = \{a_1, a_2, \ldots, a_n\}$$
(среди чисел a_i могут быть равные). Набором k-сумм назовем совокупность всех чисел вида
$$a_{i_1} + a_{i_2} + \ldots + a_{i_k}, \qquad \text{где } 1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n.$$
Обозначим этот набор $A^{(k)}$. Мы изучаем частный случай следующего основного вопроса о наборах $A^{(k)}$.

При каких (n,k) *по набору* $A^{(k)}$ *можно однозначно восстановить набор* A*?*

Опишем общий подход работ [8, 4, 3] к решению этой задачи.

В работе [4] показано, что ответ на этот вопрос не зависит от того, являются ли числа a_i целыми, вещественными или даже комплексными. Поэтому будем считать, что набор A (и $\widetilde{A}$) состоит из комплексных чисел (хотя построенный нами пример целочисленный). Рассмотрим симметрические функции набора A. Если $1 \leqslant j \leqslant n$, то для каждого набора $\{p_1, p_2, \ldots, p_j\}$ из неотрицательных целых чисел обозначим через $S_{p_1,p_2,\ldots,p_j}$ мономиальную степенную сумму
$$S_{p_1,p_2,\ldots,p_j} = \sum_{D(j)} a_{i_1}^{p_1} a_{i_2}^{p_2} \ldots a_{i_j}^{p_j}, \tag{1}$$

где суммирование ведется по множеству $D(j)$, состоящему из всевозможных упорядоченных j-подмножеств $\{i_1, i_2, \ldots, i_j\} \subset \{1, \ldots, n\}$. В частности,

$$S_p = \sum_{i=1}^{n} a_i^p.$$

Следующее соображение позволяет снизить громоздкость вычислений. Заметим, что сдвиги $\{a_1, \ldots, a_n\} \mapsto \{a_1 + t, \ldots, a_n + t\}$ и масштабирования $\{a_1, \ldots, a_n\} \mapsto \{ta_1, \ldots, ta_n\}$ не влияют на разрешимость исходной задачи. Поэтому можно считать, что $S_1 = 0$, $S_2 = 1$.

Как известно, набор степенных сумм S_p, $p = 1, 2, \ldots, n$, однозначно определяет набор A. При $m > n$ степенные суммы S_m могут быть выражены через $S_1, \ldots, S_n$ последовательным применением формулы, которую можно найти в учебнике Мак-Магона [6, стр. 6]:

$$\frac{1}{m} S_m = \sum_{\substack{1p_1 + 2p_2 + \ldots = m \\ p_m = 0}} (-1)^{\sum p_i} \frac{S_1^{p_1} S_2^{p_2} \ldots}{1^{p_1} 2^{p_2} \ldots p_1! p_2! \ldots}. \tag{2}$$

Мономиальные степенные суммы $S_{p_1, p_2, \ldots, p_j}$ также выражаются через $S_1, \ldots, S_n$ последовательным применением формулы, которая сразу следует из их определения (1):

$$\begin{aligned} &S_{p_1, p_2, \ldots, p_j} \\ &\quad = S_{p_1, p_2, \ldots, p_{j-1}} S_{p_j} - S_{p_1 + p_j, p_2, \ldots, p_{j-1}} - \ldots - S_{p_1, p_2, \ldots, p_{j-1} + p_j}. \end{aligned} \tag{3}$$

Рассмотрим теперь симметрические функции набора $A^{(k)}$. Пусть E_p – p-я степенная сумма набора $A^{(k)}$, в определении которой мы сразу раскроем скобки (напомним, что в нашем случае $k = 4$):

$$\begin{aligned} 4! E_p &= \sum_{D(4)} (a_{i_1} + a_{i_2} + a_{i_3} + a_{i_4})^p \\ &= \sum_{p_1 + p_2 + p_3 + p_4 = p} \frac{p!}{p_1! p_2! p_3! p_4!} S_{p_1, p_2, p_3, p_4}. \end{aligned} \tag{4}$$

Применяя формулы понижения (3) и (2), можно выразить функции E_p через $S_1, \ldots, S_n$, в результате получаются следующие уравнения (они приведены в статье [3]):

$$E_1 = 0, \tag{5}$$
$$E_2 = 120S_2, \tag{6}$$
$$E_3 = 48S_3, \tag{7}$$
$$E_4 = -48S_4 + 84S_2^2, \tag{8}$$
$$E_5 = -120S_5 + 140S_2S_3, \tag{9}$$
$$E_6 = 0S_6 + 40S_3^2 - 120S_2S_4 + 90S_2^3, \tag{10}$$
$$E_7 = 648S_7 - 714S_2S_5 - 350S_3S_4 + 420S_2^2S_3, \tag{11}$$
$$E_8 = 1632S_8 - 896S_2S_6 - 1120S_3S_5 - 280S_4^2 + 560S_2S_3^2 + 105S_2^4, \tag{12}$$
$$\begin{aligned} E_9 = {} & -3480S_9 + 4824S_2S_7 + 1176S_3S_6 \\ & + 1764S_4S_5 - 3024S_2^2S_5 - 2520S_2S_3S_4 + 1260S_2^3S_3, \end{aligned} \tag{13}$$
$$\begin{aligned} E_{10} = {} & -59520S_{10} + 42840S_2S_8 + 29280S_3S_7 + 23520S_4S_6 \\ & - 15120S_2^2S_6 - 8400S_3^2S_4 + 3150S_2^3S_4 \\ & - 9450S_2S_4^2 + 6300S_2^2S_3^2 - 25200S_2S_3S_5 + 12600S_5^2, \end{aligned} \tag{14}$$
$$\begin{aligned} E_{11} = {} & -407352S_{11} + 222530S_2S_9 + 196350S_3S_8 + 155100S_4S_7 \\ & - 120120S_2S_3S_6 + 150612S_5S_6 - 97020S_2S_4S_5 \\ & - 55440S_3^2S_5 + 6930S_2^3S_5 - 55440S_2^2S_7 \\ & - 46200S_3S_4^2 + 34650S_2^2S_3S_4 + 15400S_2S_3^3, \end{aligned} \tag{15}$$
$$\begin{aligned} E_{12} = {} & -2203488S_{12} + 964128S_2S_{10} + 998800S_3S_9 + 827640S_4S_8 \\ & - 178200S_2^2S_8 - 459360S_2S_3S_7 + 744480S_5S_7 + 373296S_6^2 \\ & - 415800S_2S_4S_6 - 258720S_3S_3S_6 + 13860S_2^3S_6 \\ & - 182952S_2S_5^2 - 443520S_3S_4S_5 + 83160S_2^2S_3S_5 \\ & - 69300S_4^3 + 51975S_2^2S_4^2 + 138600S_2S_3^2S_4 + 15400S_3^4. \end{aligned} \tag{16}$$

Отметим, что коэффициент перед S_6 в уравнении (10) равен нулю – именно благодаря этому обстоятельству случай $(12, 4)$ является сложным. Если бы коэффициент был ненулевым, мы последовательно нашли бы из уравнений (6)–(16) величины $S_2, \dots, S_{12}$ и однозначно восстановили исходный набор A.

Так как уравнение (10) оказалось несодержательным, Дж. Ивелл добавляет к системе еще одно уравнение

$$\begin{aligned}
E_{14} = {} & -48517440S_{14} + 14260792S_2S_{12} + 18521776S_3S_{11} \\
& + 17649632S_4S_{10} - 1513512S_2^2S_{10} - 5005000S_2S_3S_9 \\
& + 15095080S_5S_9 + 14030016S_6S_8 - 5675670S_2S_4S_8 \\
& - 3723720S_3^2S_8 + 45045S_2^3S_8 + 7008144S_7^2 - 5045040S_2S_5S_7 \\
& - 7687680S_3S_4S_7 - 2270268S_2S_6^2 + 360360S_2^2S_3S_7 \\
& - 6726720S_3S_5S_6 - 3783780S_4^2S_6 + 630630S_2^2S_4S_6 \\
& + 840840S_2S_3^2S_6 - 3531528S_4S_5^2 + 378378S_2^2S_5^2 \\
& + 2522520S_2S_3S_4S_5 + 560560S_3^3S_5 \\
& + 525525S_2S_4^3 + 1051050S_3^2S_4^2. \qquad (17)
\end{aligned}$$

Подставим в него выражение для S_{14} через $S_2, \ldots, S_{12}$ по формуле (2) и далее последовательно исключим из системы (6)–(17) переменные $S_2, \ldots, S_5$, $S_7, \ldots, S_{12}$. Благоприятным обстоятельством здесь является то, что переменные $S_2, \ldots, S_5$ непосредственно выражаются из уравнений (6)–(9) через величины E_i, а переменные $S_7, \ldots, S_{12}$ выражаются как полиномы от S_6 с коэффициентами, зависящими от E_i. В итоге получается уравнение

$$\begin{aligned}
E_{14} = {} & \left(\frac{73458}{5465}E_2\right)S_6^2 + \left(\frac{22556178701}{5315943600}E_3E_5 - \frac{889}{12}E_8 - \frac{15211}{13392}E_4^2\right. \\
& + \frac{4783550233}{\underline{\underline{119441640960}}}E_2^2E_4 - \frac{9881683541849}{\underline{418343497545600}}E_2E_3^2 \\
& \left. - \frac{72629302403}{\underline{477766563840000}}E_2^4\right)S_6 + \ldots . \qquad (18)
\end{aligned}$$

Здесь выражение, обозначенное многоточием, зависит только от параметров E_i, а подчеркнутые коэффициенты не совпадают в нашем вычислении с коэффициентами из [3]. Точные значения коэффициентов не столь существенны, но в рассуждениях о числе корней этого уравнения (относительно S_6) Ивелл пользуется тем, что коэффициент, подчеркнутый два раза, относительно велик, из-за чего уравнение может иметь лишь один положительный корень, что и дает однозначность восстановления набора A. В наших вычислениях этот коэффициент примерно в 3000 раз меньше, чем у Ивелла, и на простом примере видно, что уравнение может иметь два положительных корня.

Пример. Пусть $A = \{-1, 0^{10}, 1\}$, тогда $A^{(4)} = \{-1^{120}, 0^{255}, 1^{120}\}$. При нечетном i степенные суммы E_i равны 0, при четном i имеем $E_i = 240$. Подставив эти числа в уравнение (18), получаем два положительных корня $S_6 = 2$ и $S_6 = 377762/44361$, что противоречит утверждению [3, Theorem 2].

3. Доказательство теоремы 1. Рассмотрим наборы

$$A' = \{0, 0, 1, -1, 2, -2, 4, -4, 7, -7, 7, -7\}$$

и

$$A'' = \{1, -1, 2, -2, 3, -3, 4, -4, 5, -5, 8, -8\}.$$

Непосредственно проверяется, что наборы $(A')^{(4)}$ и $(A'')^{(4)}$ совпадают.

4. Некоторые подробности. В этом разделе мы объясняем, каким образом были найдены указанные выше наборы чисел. В вычислениях использовалась система компьютерной алгебры Maple.

Мы хотим найти два набора $A' = \{a'_1, \dots, a'_{12}\}$ и $A'' = \{a''_1, \dots, a''_{12}\}$, у которых наборы 4-сумм совпадают. Как отмечалось, можно считать, что $S'_1 = 0$, $S'_2 = 1$. Пусть S'_p, S''_p – p-е степенные суммы этих наборов, E_p – степенные суммы их общего набора 4-сумм $(A')^{(4)}$. Пользуясь уравнениями (6), (7), ..., выразим $E_2, E_3, \dots$ через $S'_1, \dots, S'_{12}$.

Теперь заново рассмотрим систему уравнений (6), (7), ..., считая, что правые части уравнений этой системы заданы с помощью вычисления из предыдущего абзаца. Работая с этой системой, k-м уравнением будем считать то, у которого в правой части находится E_k, а также следствия из этого уравнения, полученные подстановкой в него каких-либо величин. Таким образом, (6) – это 2-е уравнение, (16) – 12-е, и т.д. Для дальнейшего нам понадобятся уравнения с 1-го по 26-е.

Итак, мы имеем 26 уравнений относительно переменных S_i, причем мы подставили в эти уравнения вместо E_i их выражения через числа S'_1, ..., S'_{12}. Теперь для уравнений с 13-го по 26-е выполним такие же преобразования, как у Ивелла, а именно: последовательно выразим S_{13}, S_{14}, ..., S_{26} через S_2, ..., S_{12} по формуле (2) и далее, пользуясь уравнениями (6)–(16), исключим переменные $S_2, \dots, S_5$,

$S_7, \ldots, S_{12}$. Так, например, 14-е уравнение станет квадратным уравнением относительно S_6, оно отличается от (18) лишь тем, что все E_i выражены через S'_j. Корнями 14-го уравнения относительно единственного неизвестного S_6 должны быть числа S'_6 и S''_6. И действительно, подстановка $S = S'_6$ тождественно обнуляет 14-е уравнение, и в силу этого второй возможный корень $S_6 = S''_6$ относительно несложно выражается через $S'_1, \ldots, S'_{12}$ (здесь уже сделана подстановка $S_1 = 0$, но еще не подставлено $S_2 = 1$):

$$S''_6 = -\frac{556877605}{796368672}{S'_2}^3 + \frac{562115611087}{46487926782}{S'_3}^2 + \frac{762093077}{66364056}S'_2S'_4$$
$$-\frac{1990577}{47223}S'_6 - \frac{4217456129563}{116219816955}\cdot\frac{S'_3S'_5}{S'_2} - \frac{14623247}{1301256}\cdot\frac{{S'_4}^2}{S'_2} + \frac{2359787}{31482}\frac{S'_8}{S'_2}.$$

Найденный корень должен удовлетворять и остальным 13 уравнениям – с 15-го по 26-е и 13-му. Мы подставили его в эти уравнения (сократив их предварительно на $S_6 - S'_6$), получилось 13 полиномиальных соотношений на величины $S'_3, \ldots, S'_{12}$. Они весьма громоздки: первое представляет собой сумму 10 одночленов, последнее – сумму 130 одночленов.

Отметим еще одно соображение, слегка снижающее объем вычислений. Как нетрудно проверить, 13-е уравнение линейно относительно S_6. Оно может иметь два различных корня только в том случае, когда коэффициент при S_6 равен нулю. Это условие позволяет выразить S'_7 через S'_3, S'_4, S'_5 и тем самым уменьшить на 1 количество переменных:

$$S'_7 = -\frac{1494661249487}{4501080325368}S'_3{S'_2}^2 + \frac{217002961}{417230286}S'_2S'_5 + \frac{3678199}{2599908}S'_3S'_4.$$

В результате этой подстановки остается система из 12 уравнений, полученных из уравнений с 15-го по 26-е. Базис Грёбнера этой системы уравнений относительно невелик. Как показывает Maple, система имеет всего два решения – то, из которого получены наборы, предъявленные выше, и еще одно “самодвойственное” решение, для которого $S''_6 = S'_6$.

Литература

1. Д. В. Фомин, О. Т. Ижболдин, *Наборы кратных сумм.* — Труды С.-Петербургского мат. общества **3** (1994), 244–259.

2. J. Boman, L. Svante, *Examples of non-uniqueness for the combinatorial Radon transform modulo the symmetric group*. — Math. Scand. **78** (1996), 207–212.
3. J. A. Ewell, *On the determination of sets by sets of sums of fixed order*. — Canad. J. Math. **20** (1968), 596–611.
4. A. S. Fraenkel, B. Gordon, E. G. Straus, *On the determination of sets by the sets of sums of a certain order*. — Pacific J. Math. **12** (1962), 187–196.
5. R. K. Guy, *Unsolved Problems in Number Theory*, Springer, New York, 1994.
6. P. A. MacMahon, *Combinatorial Analysis*, Chelsea, New York, 1960.
7. L. Moser, *Problem E*1248. — Amer. Math. Monthly **64** (1957), 507.
8. J. L. Selfridge, E. G. Straus, *On the determination of numbers by their sums of a fixed order*. — Pacific J. Math. **8** (1958), 847–856.

Isomurodov J. E., Kokhas K. P. A set of 12 numbers is not determined by its set of 4-sums.

We present two sets of 12 integers that have the same sets of 4-sums. The proof of the uniqueness of determination of a set of 12 numbers by its set of 4-sums published 50 years ago is wrong, and we demonstrate an incorrect calculation in it.

С.-Петербургский
государственный университет;
ИТМО, С.-Петербург, Россия

Поступило 4 октября 2016 г.

С.-Петербургский
государственный университет,
С.-Петербург, Россия
E-mail: kpk@arbital.ru