*Информационные процессы, Том 15, № 3, 2015, стр. 337–342*




# Новый алгоритм решения комбинаторной задачи о разбиении множества [1]

**В. А. Любецкий, А. В. Селиверстов**

*Институт проблем передачи информации им. А. А. Харкевича РАН, г. Москва, Россия*
Поступила в редколлегию 07.09.2015

**Аннотация**—Предлагается новый эффективный алгоритм решения задачи о разбиении множества, у которого заданы веса элементов, на равные части. Алгоритм связан с вычислением линейной группы, сохраняющей инвариант — множество нулей кубической формы. Также обсуждаются алгоритмы решения смежных задач, включая задачу поиска второго решения, если известно первое.

**КЛЮЧЕВЫЕ СЛОВА:** алгоритм разбиения, кубическая форма, вычислительная сложность.

## 1. ЗАДАЧА О РАЗБИЕНИИ МНОЖЕСТВА И ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ

Оказывается, что многие чисто комбинаторные задачи эффективно сводятся к поиску особых точек на проективной гиперповерхности; в этом состоит новый подход авторов к их решению. В качестве примера таких комбинаторных задач рассмотрим известную задачу о разбиении на части данного множества с весами. Ниже везде рассматриваются многомерные комплексные пространства, в основном, $(n+1)$-мерное $\mathbb{C}^{n+1}$; $\mathbb{C}$ — поле комплексных чисел.

*Задача о разбиении множества.* Дано множество из $n+1$ элемента, и $j$-му элементу приписан вес $\alpha_j$ — положительное целое число. Существует ли его разбиение на две части с равными суммарными весами частей? Эта задача имеет естественный параметр: число $k$ её решений. Задачу с не более чем $k$ решениями назовём *$k$-задачей.* Само множество вместе с фиксированными весами назовём *данными* исходной задачи. Задача эквивалентна поиску вершины куба с координатами $-1$ или $+1$, лежащей на гиперплоскости с уравнением $\alpha_0 x_0 + \cdots + \alpha_n x_n = 0$. Таким образом, нужно найти вершину куба, лежащую на гиперплоскости.

Распространено мнение, что эта задача алгоритмически трудная [1, 2]. Анализ родственных задач подтверждает её высокую вычислительную сложность [3–5]. С другой стороны, для частных случаев алгоритмически трудных и близких по смыслу задач удаётся найти эффективный алгоритм [6–8]. Соотношения между верхними уровнями полиномиальной иерархии остаются мало изученными; и можно думать, что её структура существенно отличается от структуры арифметической иерархии или аналогично определяемых иерархий дескриптивной теории множеств, хотя методы их исследования основаны на сходных подходах [9–13].

В [14] показано, что задачу о разбиении множества можно свести к исследованию не только кубической, но и большей нечётной степени $d$ гиперповерхности $\alpha_0 x_0^d + \cdots + \alpha_n x_n^d = 0$. А именно, вершины куба на гиперплоскости $\alpha_0 x_0 + \cdots + \alpha_n x_n = 0$ — точки её касания с гиперповерхностью.

Другой подход состоит в том, чтобы рассматривать гиперплоское сечение гиперповерхности, которая содержит все вершины куба и каждая из них особая. Например, такова гиперповерхность, заданная уравнением четвёртой степени $g((x_0^2-1), \ldots, (x_n^2-1)) = 0$, где $g$ —

[1] Работа выполнена за счёт гранта Российского научного фонда (проект №14–50–00150).

любая невырожденная квадратичная форма от $n+1$ переменной. Произвол в выборе формы $g$ позволяет избегать появления дополнительных особых точек в гиперплоском сечении. Оценка размерности пространства гиперповерхностей фиксированной размерности, содержащих все вершины куба, дана в [15]. Рассматривая формы высших степеней, можно исследовать принадлежность к гиперплоскости не только вершин куба, но и вершин других многогранников, вложенных в комплексное пространство.

Переход от дискретных задач к исследованию гиперповерхностей позволяет получать информацию об исходной задаче путём исследования точек гиперповерхности, обладающих специальными аналитическими свойствами. Здесь видна аналогия с кодами, исправляющими ошибки[16–18]. С другой стороны, известны легко вычислимые инварианты, позволяющие эффективно различать гиперповерхности в прикладных задачах описания и распознавания объектов [19].

По определению в каждой точке *особой прямой* градиент формы равен нулю.

**Лемма 1.** *Дана кубическая форма $f$ от $n+1$ переменной. Если конус $f=0$ инвариантен относительно действия линейной группы $G=\{A,A^2\}$ в $\mathbb{C}^{n+1}$, а число особых прямых на конусе $f=0$ нечётное, то $\mathbb{C}^{n+1}$ разлагается в прямую сумму одномерного и $n$-мерного $G$-инвариантных подпространств, одно из которых содержит нечётное число особых прямых этого конуса.*

В качестве кубической формы можно рассматривать ограничение формы $\alpha_0x_0^3+\cdots+\alpha_nx_n^3$ на гиперплоскость $\alpha_0x_0+\cdots+\alpha_nx_n=0$.

*Доказательство.* Множество особых прямых, которые не остаются неподвижными при инволюции $A$, разбивается на пары прямых, переходящих одна в другую. Поскольку общее число особых прямых нечётное, то нечётно и число неподвижных особых прямых. Над $\mathbb{C}$ линейное представление абелевой группы $G$ разлагается в прямую сумму одномерных $G$-инвариантных подпространств. Возможны два случая.

1. Если действие $G$ нетривиальное, то среди одномерных $G$-инвариантных подпространств найдётся такое, чьи точки не являются $G$-инвариантными. Обозначим его через $M$. Если $M$ не совпадает с особой прямой конуса $f=0$, то все неподвижные особые прямые лежат в прямом дополнении к $M$, которое также $G$-инвариантное.
2. Если действие $G$ тривиальное, то каждая особая прямая $G$-инвариантная.

Следующая лемма усиливает в случае кубических форм результат из [14].

**Лемма 2.** *Пусть $h=\alpha_0x_0+\cdots+\alpha_nx_n$ — линейная форма с ненулевыми целыми коэффициентами от не менее чем четырёх переменных. Противоположные пары вершин куба, принадлежащие гиперплоскости $h=0$, биективно соответствуют особым прямым, по которым эта гиперплоскость касается конуса $\alpha_0x_0^3+\cdots+\alpha_nx_n^3=0$ . Более того, это — особые прямые гиперплоского сечения конуса.*

*Доказательство* состоит в непосредственном вычислении.

## 2. НОВЫЕ ГИПОТЕЗЫ

Далее речь идёт о формулах в языке теории полей с дополнительными константами для коэффициентов наперёд заданной кубической формы $f$. Эквивалентность формул рассматривается в теории алгебраически замкнутых полей нулевой характеристики.

**Лемма 3.** *Существует алгоритм полиномиального от n времени, который строит замкнутую E-формулу, истинную в* $\mathbb{C}$*, если конус* $f = 0$ *не содержит особых прямых, и ложную, если он содержит нечётное число особых прямых.*

Существование $A$-формулы, которая выражает гладкость гиперповерхности, — запись определения особой точки. Не известно: можно ли за полиномиальное время для произвольной $A$-формулы в этом языке найти эквивалентную ей $E$-формулу. Если не ограничивать сложность вычисления, то существование такой формулы очевидно. Вычислительная сложность проверки доказуемости замкнутых формул в зависимости от числа перемен кванторов подробно рассмотрена в работе [20].

*Доказательство* (набросок). Кубическая форма, определяющая конус без особых прямых, невырожденным линейным преобразованием приводится к виду $y^2z + g$, где кубическая форма $g$ не зависит от переменной $y$. В случае трёх переменных — это нормальная форма Вейерштрасса. Эта форма инвариантна относительно инволюции, меняющей знак координаты $y$. Применяя лемму 1, мы найдём особую прямую, или ограничим поиск особой прямой гиперплоским сечением $y = 0$. Если исходный конус не содержал особых прямых, то таким будет и его сечение. Поэтому для каждого сечения существует своя инволюция. Это позволяет понижать размерность, пока не останутся три переменные. Кубическая форма от трёх переменных, определяющая конус без особых прямых, невырожденным линейным преобразованием координат может быть приведена к виду $y^2z = x^3 + pxz^2 + qz^3$, где многочлен $x^3 + px + q$ не имеет кратных корней, то есть его дискриминант $-4p^3 - 27q^2$ отличен от нуля. Легко проверить, что преобразование невырожденное и приводит кубическую форму к нужному виду. И эти условия выразимы в языке теории полей.

В случае хороших приближений соответствующих комплексных чисел возникает алгоритм, позволяющий отличить гладкую кубическую поверхность от таковой с нечётным числом особых точек, выполняя полиномиально ограниченное от длины записи исходной формы число операций над этими приближениями.

**Предположение 1.** *Существует недетерминированный алгоритм полиномиального от n времени, который для каждой* 1*-задачи принимает данные, если и только если нет ни одного решения.*

Если отбросить ограничение на число решений, то предположение эквивалентно равенству $NP = coNP$, которое обычно считается ложным.

*План доказательства.* В $\mathbb{C}^{n+1}$ рассмотрим подпространство $H$, определяемое уравнением $\alpha_0x_0+\dots+\alpha_nx_n = 0$, и на нём — форму $F$, получаемую ограничением формы $\alpha_0x_0^3+\dots+\alpha_nx_n^3$. По лемме 2 нужно выяснить, имеется ли на конусе $F = 0$ в $H$ особая прямая. Используя лемму 3, найдём инволюцию $A$ и положим $G = \{A, A^2\}$. Для этого нужно недетерминированно определить значения переменных, связанных квантором существования. При этом должны появляться числа, допускающие короткую запись и аппроксимирующие соответствующие комплексные числа. Хотя в лемме 1 говорится о группе порядка 2, для уменьшения влияния погрешностей упомянутых аппроксимаций можно рассматривать бóльшую группу $G$ линейных преобразований, относительно которых конус $F = 0$ инвариантен. Построим собственное $G$-инвариантное подпространство $L$ в $H$, которому принадлежит вершина куба из $H$, если таковая существует. Если группа $G$ включает конечную подгруппу, не порождаемую малым числом элементов, то размерность подпространства $L$ мала. Действительно, по лемме 1 такое $L$ существует для подгруппы порядка 2. Если $G$ содержит две инволюции, которым соответствуют подпространства $L'$ и $L''$, то полагаем $L = L' \cap L''$. Чем больше инволюций в $G$, тем меньше размерность пересечения $L$ таких подпространств. Ещё можно использовать элементы большого порядка. В результате поиск вершины куба из $H$ сводится к решению аналогичной задачи в подпространстве меньшей размерности. В этом случае указанный процесс спуска протекает быстро. Для размерности три эта задача решается тривиально.

Для гиперповерхностей степени выше трёх известны ограничения сверху на порядок группы [21]. Тщательный анализ групп линейных преобразований, оставляющих инвариантными кубические конусы, приводит к предположению 2, которое является естественным усилением леммы 3. Например, такая группа для поверхности $x^2 + y^2 = z^3$ бесконечная.

**Предположение 2.** *Пусть $f$ — кубическая форма. Существует алгоритм полиномиального от $n$ времени, который строит замкнутую $E$-формулу свою для каждого $n$, которая в $\mathbb{C}$ выражает чётность числа особых прямых кубического конуса, если это множество конечное.*

В некоторых случаях кубическая форма приводится невырожденным линейным преобразованием координат к виду, который позволяет определять особые точки гиперповерхности, если они существуют [22, 23]. Более того, известен итерационный алгоритм для приведения к указанному виду при дополнительных условиях [24].

Возможно, изучение гиперповерхностей позволит уточнить результаты о сложности нахождения второго решения $NP$-полной задачи [25]. Действительно, если известна одна особая точка и автоморфизм гиперповерхности, то образ особой точки — также особая точка. Так поиск второй особой точки сводится к поиску автоморфизма, не оставляющего первую неподвижной.

Хотя предполагаемые алгоритмы недетерминированные, их создание позволит сертифицировать результаты вычислений на суперкомпьютерах [26]. Рост производительности вычислительных машин приводит к трудности проверки вычислений, невыполнимых на общедоступных машинах. Разработка быстрых недетерминированных алгоритмов, требующих малых памяти и времени работы, позволяет эффективно проверять результаты работы многопроцессорных вычислительных машин в случае, когда они предоставляют заказчику сертификат, содержащий все недетерминированные шаги вычисления в ходе выполнения алгоритма. В частности, это может иметь большое значение для принятия решений на транспорте [27], в области медицины [28] и при обработке изображений [29].

## СПИСОК ЛИТЕРАТУРЫ

1. Схрейвер А. *Теория линейного и целочисленного программирования.* М.: Мир, 1991. (Schrijver A. Theory of Linear and Integer Programming. Wiley, 1986.)

2. Margulies S., Onn S., Pasechnik D. V. On the complexity of Hilbert refutations for partition. *Journal of Symbolic Computation*, 2015, vol. 66, pp. 70–83.

3. Горбунов К. Ю., Селиверстов А. В., Любецкий В. А. Взаимное расположение параллельных гиперплоскостей, квадрик и вершин многомерного куба. *Проблемы передачи информации*, 2012, том 48, № 2, стр. 113–120. (*Problems of Information Transmission*, 2012, vol. 48, no. 2, pp. 185–192.)

4. Селиверстов А. В. О мономах квадратичных форм. *Дискретный анализ и исследование операций*, 2013, том. 20, № 3, стр. 65–70. (*Journal of Applied and Industrial Mathematics*, 2013, Vol. 7, no. 3, pp. 431–434.)

5. Селиверстов А. В., Любецкий В. А. О симметричных матрицах с неопределенной главной диагональю. *Проблемы передачи информации*, 2009, том 45, № 3, стр. 73–78. (*Problems of Information Transmission*, 2009, vol. 45, no. 3, pp. 258–263.)

6. Горбунов К. Ю., Любецкий В. А. Дерево, ближайшее в среднем к данному набору деревьев. *Проблемы передачи информации*, 2011, том 47, № 3, стр. 64–79. (*Problems of Information Transmission*, 2011, vol. 47, no. 3, pp. 274–288.)

7. Rusin L. Yu., Lyubetskaya E. V., Gorbunov K. Yu., Lyubetsky V. A. Reconciliation of Gene and Species Trees. *BioMed Research International*, 2014, vol. 2014, Article ID 642089.

8. Селиверстов А. В. Многогранники и связные подграфы. *Дискретный анализ и исследование операций*, 2014, том. 21, № 3, стр. 82–86.

9. Кановей В. Г., Любецкий В. А. Об эффективной $\sigma$-ограниченности и $\sigma$-компактности в модели Соловея. *Математические заметки*, 2015, том 98, № 2, стр. 247–257. (*Mathematical Notes*, 2015, vol. 98, no. 2, pp. 273–282.)

10. Kanovei V. G., Lyubetsky V. A. A definable $E_0$ class containing no definable elements. *Archive for Mathematical Logic*, 2015, vol. 54, no. 5, pp. 711–723.

11. Kanovei V. G., Lyubetsky V. A. On effective $\sigma$-boundedness and $\sigma$-compactness. *Mathematical Logic Quarterly*, 2013, vol. 59, no. 3, pp. 147–166.

12. Кановей В. Г., Любецкий В. А. Об эффективной компактности и сигма-компактности. *Математические заметки*, 2012, vol. 91, no. 6, pp. 840–852. (*Mathematical Notes*, 2012, vol. 91, no. 6, pp. 789–799.)

13. Kanovei V. G., Lyubetsky V. A. An infinity which depends on the axiom of choice. *Applied Mathematics and Computation*, 2012, vol. 218, no. 16, pp. 8196–8202.

14. Латкин И. В., Селиверстов А. В. Вычислительная сложность фрагментов теории поля комплексных чисел. *Вестник Карагандинского университета. Серия Математика*, 2015, № 1 (77), стр. 47–55.

15. Селиверстов А. В., Любецкий В. А. О формах, равных нулю в каждой вершине куба. *Информационные процессы*, 2011, том 11, №3, стр. 330–335. (*Journal of Communications Technology and Electronics*, 2012, vol. 57, no. 8, pp. 892–895.)

16. Влэдуц С. Г., Кабатянский Г. А., Ломаков В. В. Об исправлении ошибок при искажениях в канале и синдроме. *Проблемы передачи информации*, 2015, том 51, № 2, стр. 50–56. (*Problems of Information Transmission*, 2015, vol. 51, no. 2, pp. 132–138.)

17. Трифонов П. В. Декодирование кодов Рида–Соломона методом последовательного исключения. *Проблемы передачи информации*, 2014, том 50, № 4, стр. 3–14. (*Problems of Information Transmission*, 2014, vol. 50, no. 4, pp. 303–312.)

18. Жилин И. В., Крещук А. А., Зяблов В. В.Обобщённые коды с локализацией ошибок и минимизация избыточности для заданных входной и выходной вероятностей ошибки. *Информационные процессы*, 2014, том 14, № 4, стр. 370–384. (*Journal of Communications Technology and Electronics*, 2015, vol. 60, no. 6, pp. 695–706.)

19. Гершгорин Р. А., Рубанов Л. И., Селиверстов А. В. Легко вычислимые инварианты для распознавания гиперповерхности. *Информационные процессы*, 2014, том 14, № 4, стр. 365–369. (*Journal of Communications Technology and Electronics*, 2015, no. 12, in press.)

20. Григорьев Д. Ю. Сложность разрешения теории первого порядка алгебраически замкнутых полей. *Известия АН СССР. Сер. Матем.*, 1986, том 50, № 5, стр. 1106–1120. (*Mathematics of the USSR-Izvestiya*, 1987, vol. 29, no. 2, pp. 459–475.)

21. Jelonek Z., Lenarcik T. Automorphisms of affine smooth varieties. *Proc. Amer. Math. Soc.*, 2014, vol. 142, pp. 1157–1163

22. Seliverstov A. V. Cubic hypersurfaces with an odd number of singular points. *International Conference Polynomial Computer Algebra '2015, St. Petersburg, April 13–18 2015, Euler International Mathematical Institute.* VVM Publishing, 2015, pp. 85–86.

23. Селиверстов А. В. О вычислительной сложности поиска особых точек. *Дискретная математика, алгебра и их приложения: Тезисы докладов Международной научной конференции, Минск, 14–18 сентября 2015.* Минск: Институт математики НАН Беларуси, 2015, стр. 135–137.

24. Селиверстов А. В. Кубические формы без мономов от двух переменных. *Вестник Удмуртского университета. Математика. Механика. Компьютерные науки*, 2015, том 25, № 1, стр. 71–77.

25. Найденко В. Г. О сложности нахождения второго решения NP-полной задачи. *Весці Нацыянальнай Акадэміі Навук Беларусі. Серыя фізіка-матэматычных навук*, 2012, № 2, стр. 114–118.

26. Рубанов Л. И. О распараллеливании неоднородных циклов на суперкомпьютерах с распределённой памятью. *Информационные процессы*, 2013, том 13, № 4, стр. 295–305. (*Journal of Communications Technology and Electronics*, 2014, vol. 59, no. 6, pp. 639–646.)

27. Кузнецов Н. А., Пащенко Ф. Ф., Рябых Н. Г., Захарова Е. М., Минашина И. К. Алгоритмы оптимизации в задачах планирования на рельсовом транспорте. *Информационные процессы*, 2014, том 14, № 4, стр. 307–318. (*Journal of Communications Technology and Electronics*, 2015, vol. 60, no. 6, pp. 637–646.)

28. Григорьев Ф. Н., Гуляев Ю. В., Дворникова С. Н., Коздоба О. А., Кузнецов Н. А. Задача распознавания образов для диагностики сердечнососудистых заболеваний по данным ЭКГ. *Информационные процессы*, 2014, том 14, № 2, стр. 178–184. (*Journal of Communications Technology and Electronics*, 2015, vol. 60, no. 6, pp. 673–677.)

29. Чочиа П. А. Переход от 2D- к 3D-изображениям: модификация двухмасштабной модели и алгоритмов обработки. *Информационные процессы*, 2014, том 14, № 3, стр. 242–255. (*Journal of Communications Technology and Electronics*, 2015, vol. 60, no. 6, pp. 678–687.)

## A novel algorithm to solve the combinatory set partitioning problem

**Seliverstov A. V., Lyubetsky V. A.**

A novel efficient algorithm is proposed for equal partitioning of a set with predefined weights of the elements. The algorithm based on a group preserving the invariant that is the set of zeros of a cubic form. The algorithms to solve related problems including computing a second solution when the first is known are discussed.

**KEYWORDS:** algorithm for partition, cubic form, computational complexity.