ЖУРНАЛ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И МАТЕМАТИЧЕСКОЙ ФИЗИКИ, 2023, том 63, № 1, с. 51–60

ОБЩИЕ ЧИСЛЕННЫЕ МЕТОДЫ

УДК 519.161

ОБОБЩЕНИЕ ЗАДАЧИ О СУММЕ ПОДМНОЖЕСТВ И КУБИЧЕСКИЕ ФОРМЫ

© 2023 г. А. В. Селиверстов[1,*]

[1] 127051 Москва, Большой Каретный пер., 19, стр. 1, ИППИ РАН, Россия

*e-mail: slvstv@iitp.ru

Поступила в редакцию 19.04.2022 г.
Переработанный вариант 12.05.2022 г.
Принята к публикации 10.09.2022 г.

Предложен новый алгоритм для распознавания существования двоичного решения у системы линейных уравнений над полем нулевой характеристики, который эффективен при выполнении некоторого ограничения на систему уравнений. Это частный случай задачи целочисленного программирования. В расширенной версии задачи о сумме подмножеств вес может быть как положительным, так и отрицательным. Рассмотренная нами задача эквивалентна задаче о существовании решения для нескольких частных случаев этой задачи одновременно. Найдены новые достаточные условия, при которых вычислительная сложность почти всех частных случаев такой задачи полиномиальная. По сути, алгоритм проверяет, существует ли кубическая гиперповерхность, проходящая через каждую вершину единичного куба, но не пересекающая заданное аффинное подпространство. Ранее уже было известно несколько эвристических алгоритмов для решения этой задачи. Однако новые методы расширяют возможности для решения тех или иных задач. Хотя подробно рассмотрена лишь задача распознавания, бинарный поиск позволяет найти решение, если это возможно. Библ. 40.

Ключевые слова: целочисленное программирование, система линейных уравнений, сумма подмножеств, сложность в среднем.

DOI: 10.31857/S0044466923010118, **EDN:** LEEUWB

1. ВВЕДЕНИЕ

Задача о сумме подмножеств состоит в распознавании существования {0,1}-решения у линейного уравнения. Она служит одним из хорошо известных примеров NP-полных задач. Задача с n переменными разрешима посредством $O(2^{n/2})$ арифметических операций (см. [1]). Общепринятая гипотеза утверждает, что для решения этой задачи в худшем случае требуется экспоненциальное время. Эта нижняя оценка была проверена для некоторых вычислительных моделей с ограничениями, включая так называемые линейные машины (см. [2], [3]) и аддитивные машины (см. [4]), а также для методов проверки разрешимости систем алгебраических уравнений, которые основаны на теореме о многочленах над вещественно замкнутым полем (Positivstellensatz) (см. [5]) или на теореме Гильберта о нулях (Nullstellenzatz) (см. [6]). С другой стороны, эта задача может быть решена за псевдополиномиальное время методом динамического программирования (см. [7], [8]). Также известны эвристические алгоритмы для случая низкой плотности (см. [9], [10]). Эта задача также допускает обобщение над кольцами вычетов (модулярный случай) (см. [11]) и над мультипликативными полугруппами матриц (см. [12]).

Мы рассмотрим задачу о существовании {0,1}-решения у системы линейных уравнений. В худшем случае вычислительная сложность этой задачи такая же, как и для задачи о сумме подмножеств, когда рассматривается одно уравнение. Однако быстрые эвристические алгоритмы известны для систем из достаточно большого числа уравнений с ограничением на знаки коэффициентов (см. [13], [14]), с коэффициентами любого знака (см. [15]) или при выполнении некоторых других ограничений (см. [16], [17]). Обзор некоторых алгоритмов дан в следующем разделе.

Известны эвристические методы решения или аппроксимации близких задач оптимизации, включая задачу о многомерном рюкзаке (см. [18], [19]), модулярный вариант этой задачи (см. [20]) и смешанные задачи о рюкзаке и покрытии (см. [21]). Для их решения тоже применимы об-

щие методы оптимизации (см. [22], [23]). Также известны эвристические алгоритмы, основанные на локальном поиске, для проверки выполнимости пропозициональной конъюнктивной нормальной формы (КНФ) (см. [24], [25]), в частности, 3-КНФ (см. [26]). Этот же метод позволяет решать соответствующую задачу оптимизации (см. [27]). С другой стороны, известна лишь экспоненциальная верхняя оценка $O^*(1.2989^m)$ на сложность в худшем случае задачи о максимальном числе одновременно выполнимых элементарных дизъюнкций в составе КНФ с m элементарными дизъюнкциями (см. [28]). Задача о выполнимости КНФ эквивалентна существованию $\{0,1\}$-решения у системы линейных неравенств от такого же числа переменных над упорядоченным кольцом целых чисел. Поэтому оценки сложности в худшем случае для этих задач связаны друг с другом.

Говоря о вычислительной сложности в среднем, мы предполагаем, что на множестве входов произвольно фиксированной длины задана вероятностная мера. Обычно каждое такое множество конечное, следовательно, все входы в нем могут быть равновероятными. Сложностью в среднем называется математическое ожидание вычислительной сложности на входах данной длины (см. [29]).

Основной результат настоящей статьи в том, что предложен эвристический алгоритм для задачи распознавания систем линейных уравнений, не имеющих $\{0,1\}$-решения. Он применим при более слабых ограничениях, чем было ранее. Также он может использоваться параллельно с другими методами. Результаты справедливы над произвольным полем характеристики нуль, операции в котором эффективно вычислимые. Чтобы упростить изложение, обычно рассматриваются вычисления над полем рациональных чисел или над чисто трансцендентным расширением этого поля. Однако можно эффективно проводить вычисления с алгебраическими числами (см. [30]), используя алгоритмы для работы с многочленами (см. [31]).

2. ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ

Рассмотрим систему из m линейных уравнений от $n > m$ переменных. Исключая переменные, легко получить новое уравнение от $n - m$ переменных. Если $n - m = O(\log_2 n)$, задача поиска $\{0,1\}$-решения для исходной системы уравнений разрешима за полиномиальное время. Она сводится к поиску каждого $\{0,1\}$-решения для уравнения от $O(\log_2 n)$ переменных и проверке, продолжается ли оно до $\{0,1\}$-решения исходной системы. Далее рассмотрены менее тривиальные случаи, когда эта задача легко разрешима.

Обозначим через $\mathbf{b}$ столбец и через A прямоугольную $m \times n$ матрицу с неотрицательными элементами. Все $\{0,1\}$-решения системы неравенств $A\mathbf{x} \leqslant \mathbf{b}$ можно найти методом динамического программирования, время работы которого мало, если общее число таких решений мало. Н.Н. Кузюрин в [13], [14] показал, что при $m > 9\log_2 n$ и некоторых предположениях о распределении элементов матрицы A и столбца $\mathbf{b}$ среднее число таких решений ограничено сверху многочленом от n. Следовательно, среднее время работы алгоритма также полиномиальное. Доказательство основано на оценке хвоста биномиального распределения. Зная все решения системы неравенств, среди них легко выбрать решение для системы уравнений, если оно существует. Важным ограничением применимости этого метода служит требование неотрицательности элементов матрицы A. Заменами переменных типа $y_k = 1 - x_k$ систему уравнений с произвольными коэффициентами легко свести к системе уравнений с неотрицательными коэффициентами у линейных членов, где новая и исходная системы имеют равное число $\{0,1\}$-решений. Но при этом искажается исходное распределение коэффициентов.

Для системы из m линейных уравнений от n переменных с положительными целыми коэффициентами a_k определим плотность по формуле

$$\varrho = \frac{n}{m\log_2 \max\limits_k a_k}.$$

При $m = 1$ и при условии малой плотности $\varrho < 0.9408$ почти все частные случаи задачи о сумме подмножеств разрешимы за полиномиальное время, используя поиск кратчайшего ненулевого вектора в некоторой решетке (см. [9], [10]). Этот метод обобщается на случай систем многих уравнений с тем же ограничением на плотность (см. [16]).

Следуя работам [15] и [32], для оценки доли входов данного размера, на которых алгоритм быстро принимает правильное решение, мы используем лемму Шварца–Зиппеля (см. [33]).

Лемма 1. *Дан отличный от константы многочлен $f(x_1,\ldots,x_n)$ степени d над полем K. Если случайные величины ξ_1, ..., ξ_n независимы и равномерно распределены на конечном множестве $S \subseteq K$ мощности $|S|$, то выполнено неравенство*

$$\Pr[f(\xi_1,\ldots,\xi_n) = 0] \leqslant \frac{d}{|S|},$$

где через $\Pr[\cdot]$ *обозначена вероятность выполнения условия в квадратных скобках.*

Недавно этот результат был усилен для многочленов от одной переменной над полем комплексных чисел. Существует такое множество из $2d+1$ чисел, что любые два многочлена f и g степени d равны друг другу, когда множество значений многочлена f вложено во множество значений многочлена g на этом множестве (см. [34]).

Ранг матрицы над полем можно вычислить, используя полиномиальное число процессоров и выполнив на каждом из них лишь $O(\log_2^2 n)$ операций над этим полем (см. [35], [36]). С другой стороны, верхние оценки сложности вычисления ранга матрицы близки к сложности матричного умножения (см. [37], [38]). В настоящей работе примеры вычислены в системе компьютерной алгебры MathPartner (см. [39]). Определитель матрицы вычисляется командой \det(), а ранг – командой \rank(). В системе Maple определитель, ранг и перманент матрицы вычислимы, например, в пакете LinearAlgebra.

3. РЕЗУЛЬТАТЫ

Геометрический смысл задачи состоит в проверке, проходит ли аффинное подпространство, заданное системой линейных уравнений, через некоторую вершину единичного n-мерного куба. Каждая такая вершина соответствует $\{0,1\}$-решению. Метод состоит в попытке построить алгебраическую гиперповерхность малой степени, проходящую через каждую вершину единичного куба, но не пересекающую данное аффинное подпространство. Здесь гиперповерхность может быть приводимой. Существование такой гиперповерхности влечет отсутствие $\{0,1\}$-решения у исходной системы уравнений. Вычислительная сложность этого метода зависит от степени гиперповерхности. Ранее было исследовано применение квадрик для случая подпространств малой размерности (см. [15]). С другой стороны, для общей гиперплоскости объединение из 2^n параллельных гиперплоскостей, содержащих все вершины единичного n-мерного куба, служит искомой гиперповерхностью степени не выше 2^n. Но степень может быть ниже. В частности, если гиперплоскость задана уравнением с ограниченными сверху положительными целыми коэффициентами, которое не имеет $\{0,1\}$-решений, то достаточно малого числа параллельных гиперплоскостей. На этом основан метод динамического программирования для решения задачи о сумме подмножеств. Однако мы рассматриваем произвольные гиперповерхности, которые не обязательно служат объединением гиперплоскостей.

3.1. Прямые на проективной плоскости

Сначала мы рассмотрим прямую на плоскости, что соответствует поиску $\{0,1\}$-решения неоднородного линейного уравнения от двух переменных x_1 и x_2. Его гомогенизацией служит уравнение от трех переменных x_0, x_1 и x_2. Каждое $\{0,1\}$-решение соответствует вершине единичного квадрата. На проективной плоскости эти вершины имеют однородные координаты $(1:0:0)$, $(1:0:1)$, $(1:1:0)$ и $(1:1:1)$ соответственно. В этих координатах бесконечно удаленная прямая задана уравнением $x_0 = 0$. Проективная кривая определяется тернарной формой (однородным многочленом), которая обращается в нуль в точках кривой.

Теорема 1. *Дан квадрат на проективной плоскости. Прямая L не проходит через какую-либо вершину квадрата тогда и только тогда, когда существует кубическая кривая, проходящая через каждую вершину квадрата, но пересекающая прямую L лишь в точке на бесконечно удаленной прямой.*

Доказательство. Пусть однородные координаты вершин квадрата (1 : 0 : 0), (1 : 0 : 1), (1 : 1 : 0) и (1 : 1 : 1). Проективная кубическая кривая определяется тернарной кубической формой. Такая форма, обращающаяся в нуль в каждой вершине квадрата, равна линейной комбинации шести форм $x_k x_j(x_j - x_0)$, где $k \in \{0,1,2\}$ и $j \in \{1,2\}$. Эти формы линейно независимые. Поэтому размерность линейного пространства кубических форм, обращающихся в нуль в каждой вершине квадрата, равна шести (см. [40]). Размерность пространства всех бинарных кубических форм равна четырем. Ограничение формы на прямую L определяет линейное отображение π из пространства тернарных форм, которые обращаются в нуль в каждой вершине квадрата, в пространство всех бинарных форм. Ядро отображения π состоит из форм, тождественно равных нулю на прямой L. Каждая форма из ядра приводимая и делится на линейную форму ℓ, определяющую прямую L. Поскольку по предположению прямая L не проходит через какую-либо вершину квадрата, то размерность ядра равна размерности квадратичных тернарных форм, обращающихся в нуль в каждой вершине квадрата. Согласно [40], это формы типа $\lambda_1 x_1(x_1 - x_0) + \lambda_2 x_2(x_2 - x_0)$. Поэтому размерность ядра отображения π равна двум. Следовательно, размерность образа отображения π совпадает с размерностью всех бинарных форм. Отображение π сюръективное. В частности, образом некоторой кубической формы $c(x_0, x_1, x_2)$ из области определения π служит форма x_0^3. Уравнение $c(x_0, x_1, x_2) = 0$ определяет кривую, которая пересекает прямую L лишь в бесконечно удаленной точке. Более того, поскольку размерность ядра равна двум, то существует однопараметрическое семейство таких кривых.

Это рассуждение существенно использует предположение, что прямая L не проходит через какую-либо вершину квадрата. Иначе ядру отображения π принадлежали бы произведения линейной формы ℓ и некоторой квадратичной формы, которая обращается в нуль лишь в трех вершинах квадрата. Тогда размерность ядра больше двух, а отображение π несюръективное. Очевидно, в этом случае прямая L пересекает каждую кривую из области определения π в некоторой вершине квадрата. Теорема доказана.

В теореме 1 кубическую кривую нельзя заменить на конику. Действительно, тернарные квадратичные формы, обращающиеся в нуль в каждой вершине квадрата, порождают линейное пространство размерности два, но бинарные квадратичные формы порождают пространство размерности три. Поэтому аналог отображения π из доказательства теоремы 1 уже не будет сюръективным.

3.2. Линейные пространства форм

Размерность линейного пространства форм степени d от переменных $x_0, \ldots, x_s$ равна биномиальному коэффициенту $\binom{s+d}{d}$. Рассмотрим линейные комбинации кубических форм типа $x_k(x_k - x_0)x_t$. Каждая такая форма обращается в нуль в каждой точке с координатами $x_0 = 1$ и $x_k \in \{0,1\}$, где $1 \leqslant k \leqslant n$. Ограничение этих форм на линейное подпространство, определяемое системой уравнений $x_j = \ell_j(x_0, \ldots, x_s)$, где $s < j \leqslant n$, равно линейной комбинации форм двух типов: либо $x_k(x_k - x_0)x_t$, либо $\ell_j(\ell_j - x_0)x_t$, где $1 \leqslant k \leqslant s$ и $0 \leqslant t \leqslant s$.

Лемма 2. *Дан набор линейных форм $\ell_j(x_0, \ldots, x_s) = a_{j0}x_0 + \cdots + a_{js}x_s$, где $s < j \leqslant n$ и все коэффициенты a_{ji} – алгебраически независимые элементы чисто трансцендентного расширения поля рациональных чисел степени трансцендентности $(n-s)(s+1)$. Если выполнено неравенство $(s+3)(s+2) \leqslant 6(n-s)$, то каждая кубическая форма от переменных $x_0, \ldots, x_s$ равна некоторой линейной комбинации форм типа $\ell_j^2 x_t$, где $s < j \leqslant n$ и $0 \leqslant t \leqslant s$.*

Доказательство. Обозначим через M матрицу, составленную из коэффициентов форм типа $\ell_j^2 x_t$, где столбцы соответствуют мономам, а строки – формам. Общее число форм типа $\ell_j^2 x_t$ должно быть не меньше, чем число мономов третьей степени. То есть должно выполняться неравенство

$$\frac{(s+3)!}{s!3!} \leqslant (n-s)(s+1),$$

где слева – общее число мономов третьей степени, а справа – число форм типа $\ell_j^2 x_t$. Оно эквивалентно неравенству $(s+3)(s+2) \leqslant 6(n-s)$ из условия леммы. При выполнении этого неравенства достаточно показать, что матрица M имеет полный ранг, равный числу столбцов.

Выделим в матрице M квадратную подматрицу M' с тем же числом столбцов, которая содержит набор ненулевых элементов по одному из каждой строки и каждого столбца. Определитель равен альтернированной сумме произведений элементов из наборов по одному элементу из каждой строки и каждого столбца. Чисто трансцендентное расширение поля изоморфно полю рациональных функций. Элементы матрицы M' можно рассматривать как многочлены от переменных a_{jk}, которые упорядочены в соответствии с порядком на индексах:

$$a_{(s+1)0} > a_{(s+1)1} > \cdots > a_{j0} > a_{j1} > \cdots > a_{js} > \cdots > a_{ns}.$$

Это определяет мономиальное упорядочение. Мы выбираем в матрице M' набор ненулевых элементов по одному из каждой строки и каждого столбца, для которого произведение максимально при этом мономиальном упорядочении. Этот максимум достигается на единственном наборе элементов из M'. Действительно, если два разных таких набора имеют равные произведения элементов, то можно найти третий набор, произведение элементов которого больше.

Поскольку a_{jk} алгебраически независимые, никакое их произведение не равно линейной комбинации других произведений. Следовательно, определитель матрицы M' отличен от нуля. Поэтому матрица M имеет полный ранг. Лемма доказана.

Элементы чисто трансцендентного расширения поля можно отождествить с функциями от независимых переменных a_{ji}. Лемма 2 справедлива для некоторых разреженных матриц, получаемых подстановкой целых значений переменных a_{ji}.

Пусть $n = 3$ и $s = 1$. Выберем $\ell_2 = x_0$ и $\ell_3 = x_1$. Матрица коэффициентов кубических форм типа $\ell_j^2 x_t$ невырожденная, поскольку она равна единичной 4×4 матрице. Поскольку размерность линейного пространства бинарных кубических форм равна четырем, формы типа $\ell_j^2 x_t$ порождают это пространство.

Пусть $n = 6$ и $s = 2$. Выберем $\ell_3 = x_0$, $\ell_4 = x_1$, $\ell_5 = x_2$ и $\ell_6 = x_1 + x_2$. Матрица M коэффициентов кубических форм типа $\ell_j^2 x_t$ содержит двенадцать строк и десять столбцов. Ранг матрицы M равен десяти и совпадет с размерностью линейного пространства тернарных кубических форм.

Пусть $n = 8$ и $s = 3$. Выберем $\ell_4 = x_0$, $\ell_5 = x_1$, $\ell_6 = x_2$, $\ell_7 = x_3$ и $\ell_8 = x_0 + x_1 + x_2 + x_3$. Матрица M коэффициентов кубических форм типа $\ell_j^2 x_t$ квадратная. Ранг равен двадцати и совпадет с размерностью линейного пространства кубических форм от четырех переменных.

Лемма 3. *Дан набор линейных форм $\ell_j(x_0, \ldots, x_s) = a_{j0}x_0 + \cdots + a_{js}x_s$, где $s < j \leqslant n$ и все коэффициенты a_{ji} – алгебраически независимые элементы чисто трансцендентного расширения поля рациональных чисел степени трансцендентности $(n-s)(s+1)$. Если выполнено неравенство $(s+3)(s+2) \leqslant 6(n-s)$, то каждая кубическая форма от переменных x_0, ..., x_s равна некоторой линейной комбинации форм типа $\ell_j(\ell_j - x_0)x_t$, где $s < j \leqslant n$ и $0 \leqslant t \leqslant s$.*

Доказательство. По аналогии с доказательством леммы 2, покажем, что матрица N, состоящая из коэффициентов форм типа $\ell_j(\ell_j - x_0)x_t$, имеет полный ранг. Матрица N равна сумме матрицы M, состоящей из коэффициентов форм типа $\ell_j^2 x_t$, и матрицы B, состоящей из коэффициентов форм типа $-x_0\ell_j x_t$. Однако элементы матрицы B, рассматриваемые как многочлены от переменных a_{ji}, имеют меньшую степень, чем элементы матрицы M. Поэтому ранг матрицы $N = M + B$ не ниже ранга матрицы M. По лемме 2 матрица M имеет полный ранг. Следовательно, матрица N тоже имеет полный ранг. Лемма доказана.

Алгоритм, обсуждаемый при доказательстве Теорем 2 и 3

Вход: целые числа $0 < m < n$ и линейные формы $\ell_j(x_0,\ldots,x_{n-m})$, где $n-m < j \leqslant n$.

1: Элементами матрицы A служат коэффициенты формы

$$\sum_{t=0}^{n-m}\left(\sum_{k=1}^{n-m}\lambda_{tk}x_k(x_k-x_0)+\sum_{j=n-m+1}^{n}\lambda_{tj}\ell_j(\ell_j-x_0)\right)x_t,$$

где строки матрицы A соответствуют мономам третьей степени от переменных x_0, ..., x_{n-m}, а столбцы – переменным λ_{tk} и λ_{tj};

2: Расширенная матрица B получается из матрицы A добавлением столбца, в котором единица стоит в строке, соответствующей моному x_0^3, а остальные элементы этого столбца равны нулю;

3: **if** $\operatorname{rank}(A) = \operatorname{rank}(B)$ **then** вход отвергается;

4: **else** выдается уведомление о неопределенности выбора.

3.3. Алгоритм и оценки вычислительной сложности

Говоря о задачах распознавания, мы предлагаем три варианта ответа: вход может быть не только принят или отвергнут, но также возможно явное уведомление о неопределенности выбора. При этом ответ должен быть получен за конечное время и без ошибок, а уведомление о неопределенности может быть выдано лишь на малой доле входов (см. [12], [15]).

Под вычислительной сложностью подразумевается алгебраическая сложность, которая равна числу арифметических операций с числами и сравнений чисел (см. [29]). Сложность выполнения отдельной операции не учитывается.

Теорема 2. *Существует алгоритм распознавания с тремя вариантами ответа, получающий на вход положительные целые числа n и $m < n$, а также систему из m линейных форм $\ell_j(x_0,\ldots,x_{n-m})$, где $n-m < j \leqslant n$, который при выполнении неравенства $(n-m+3)(n-m+2) \leqslant 6m$ удовлетворяет следующим условиям:*

- *алгебраическая сложность алгоритма ограничена сверху многочленом от n;*
- *если вход отвергается, то система уравнений $x_j = \ell_j(1, x_1,\ldots,x_{n-m})$ для индексов $n-m < j \leqslant n$ не имеет никакого $\{0,1\}$-решения;*
- *если вход принимается, то система уравнений $x_j = \ell_j(1, x_1,\ldots,x_{n-m})$ для индексов $n-m < j \leqslant n$ имеет $\{0,1\}$-решение;*
- *для любого допустимого набора значений n и m существует такой отличный от тождественно нулевого многочлен степени не выше $n^2(n-m+1)^2$ от коэффициентов всех линейных форм ℓ_j, что если алгоритм на некотором входе выдает уведомление о неопределенности выбора, то этот многочлен обращается в нуль для соответствующего набора значений коэффициентов.*

Доказательство. По сути, алгоритм, приведенный в настоящей работе, проверяет существование наборов чисел λ_{tk} и λ_{tj}, для которых выполнено равенство двух кубических форм

$$\sum_{t=0}^{n-m}\left(\sum_{k=1}^{n-m}\lambda_{tk}x_k(x_k-x_0)+\sum_{j=n-m+1}^{n}\lambda_{tj}\ell_j(\ell_j-x_0)\right)x_t = x_0^3.$$

Здесь $0 \leqslant t \leqslant n-m$. Эта проверка сводится к решению системы линейных уравнений относительно λ_{tk} и λ_{tj}. Общее число переменных в этой системе не превышает $n(n-m+1)$. Каждое уравнение в этой системе соответствует очередному моному третьей степени от переменных x_0, ..., x_{n-m}. Поэтому число этих уравнений равно $(n-m+1)(n-m+2)(n-m+3)/6$. При выполнении неравенства из условия теоремы, число уравнений этой системы не превосходит числа переменных λ_{tk} и λ_{tj}. По теореме Кронекера–Капелли решение существует при совпадении рангов двух матриц. При этом расширенная матрица получается добавлением столбца, в котором равны нулю все элементы, кроме одного. Ранг матрицы легко вычисляется. Элементами этих матриц слу-

жат многочлены степени не выше второй от коэффициентов линейных форм ℓ_j. Достаточным условием существования решения служит отличие от нуля минора, равного многочлену степени не выше $n^2(n-m+1)^2$ от коэффициентов линейных форм ℓ_j. По лемме 3 этот многочлен не обращается в нуль тождественно. Теорема доказана.

Если алгоритм из теоремы 2 отвергает систему уравнений S, то он отвергает и любую систему уравнений S', которая получена добавлением к S новых уравнений.

При сравнении теорем 1 и 2 видно, что условие в теореме 2 неоптимальное при $n = 2$. В частности, это связано с грубой оценкой ранга матрицы в доказательстве леммы 3.

Теорема 3. *Существует алгоритм распознавания с тремя вариантами ответа, получающий на вход положительные целые числа n и $m < n$, а также систему из m линейных форм $\ell_j(x_0,\ldots,x_{n-m})$, где $n-m < j \leqslant n$, который при выполнении неравенства $(n-m+3)(n-m+2) \leqslant 6m$ удовлетворяет следующим условиям*:

• *алгебраическая сложность алгоритма ограничена сверху многочленом от n*;

• *если вход отвергается, то система уравнений $x_j = \ell_j(1, x_1,\ldots,x_{n-m})$ для индексов $n-m < j \leqslant n$ не имеет никакого $\{0,1\}$-решения*;

• *если вход принимается, то система уравнений $x_j = \ell_j(1, x_1,\ldots,x_{n-m})$ для индексов $n-m < j \leqslant n$ имеет $\{0,1\}$-решение*;

• *для любого рационального числа ε из интервала $0 < \varepsilon < 1$ и для любых допустимых значений n и m, если все коэффициенты форм ℓ_j независимо и равномерно распределены на множестве мощности не меньше $(1/\varepsilon)n^2(n-m+1)^2$, то вероятность выдачи уведомления о неопределенности выбора не превышает числа ε*.

Доказательство. Применяем, как и при доказательстве теоремы 2, алгоритм, представленный в настоящей работе. Существует отличный от тождественно нулевого многочлен степени не выше $n^2(n-m+1)^2$ от коэффициентов всех линейных форм ℓ_j, который обращается в нуль на тех наборах, на которых выдается уведомление о неопределенности выбора. По лемме Шварца–Зиппеля (лемма 1) вероятность обращения этого многочлена в нуль не превышает числа ε. Теорема доказана.

4. ЗАКЛЮЧЕНИЕ

Неравенство из теорем 2 и 3 имеет вид $m \geqslant n - \sqrt{6n - o(n)}$. Аналогичное условие в ранее опубликованном алгоритме [15], использующем не кубические, а квадратичные формы, имело вид $m \geqslant n - \sqrt{2n - o(n)}$. Поэтому новый алгоритм применим при меньших ограничениях. С другой стороны, поскольку в основе работы алгоритма лежит вычисление ранга матрицы, вычисления могут быть эффективно реализованы на многопроцессорных вычислительных устройствах.

Предлагаемый алгоритм не обеспечивает полиномиальную вычислительную сложность в худшем случае. Но для многих случаев он гораздо эффективнее полного перебора. Если коэффициенты при линейных членах уравнений положительные, то в среднем более эффективен алгоритм, который предложил Н.Н. Кузюрин (см. [13], [14]). Однако новый алгоритм может быть эффективнее в случае коэффициентов разных знаков.

Существуют различные пути сведения данной системы линейных уравнений к другой такой системе, имеющей столько же $\{0,1\}$-решений. Это открывает дополнительные возможности преодолеть неопределенность ответа. С другой стороны, хотя рассмотрена лишь задача распознавания, бинарный поиск позволяет искать само $\{0,1\}$-решение, если оно существует. В частности, доказательство отсутствия $\{0,1\}$-решения, соответствующего вершине какой-либо фасете единичного куба, позволяет уменьшить число переменных в исходной задаче. То же справедливо, если вместо фасеты рассматривать пару симметрично расположенных граней коразмерности два, лежащих в одной гиперплоскости. На этом пути возможно комбинированное применение разных методов на разных шагах.

Рассмотренный в настоящей статье алгоритм никогда не принимает вход. Но используя другие известные методы, включая алгоритм Кузюрина, можно уменьшить число уведомлений об отказе. После этого новый алгоритм может принимать некоторые входы.

Хорошо известна близкая NP-полная задача о выполнимости 3-КНФ, для решения которой известны эвристические алгоритмы и их программные реализации. Хотя последняя задача также сводится за полиномиальное время к задаче о сумме подмножества, для решения задачи о выполнимости 3-КНФ новый предлагаемый алгоритм, вероятно, не даст выигрыша для практически применимых размеров входа. Однако новый алгоритм применим к более широкому набору частных задач. Это увеличивает интерес к обобщениям задачи о сумме подмножества, а не только к задаче о выполнимости 3-КНФ.

Автор благодарен М.Д. Малых и анонимному рецензенту за полезные замечания.

СПИСОК ЛИТЕРАТУРЫ

1. *Horowitz E., Sahni S.* Computing partitions with applications to the knapsack problem // J. ACM. 1974. V. 21. № 2. P. 277–292. https://doi.org/10.1145/321812.321823
2. *Meer K.* A note on a $P \neq NP$ result for a restricted class of real machines // J. Complexity. 1992. V. 8. № 4. P. 451–453. https://doi.org/10.1016/0885-064X(92)90007-X
3. *Koiran P.* Computing over the reals with addition and order // Theoret. Comput. Sci. 1994. V. 133. № 1. P. 35–47. https://doi.org/10.1016/0304-3975(93)00063-B
4. *Cucker F., Matamala M.* On digital nondeterminism // Math. Systems Theory. 1996. V. 29. P. 635–647. https://doi.org/10.1007/BF01301968
5. *Grigoriev D.* Complexity of Positivstellensatz proofs for the knapsack // Comput. Complexity. 2001. V. 10. P. 139–154. https://doi.org/10.1007/s00037-001-8192-0
6. *Margulies S., Onn S., Pasechnik D.V.* On the complexity of Hilbert refutations for partition // J. Symbolic Comput. 2015. V. 66. P. 70–83. https://doi.org/10.1016/j.jsc.2013.06.005
7. *Koiliaris K., Xu C.* Faster pseudopolynomial time algorithms for subset sum // ACM Trans. Algorithms. 2019. V. 15. № 3. Article 40. P. 1–20. https://doi.org/10.1145/3329863
8. *Polak A., Rohwedder L., Wegrzycki K.* Knapsack and subset sum with small items // In: Bansal N., Merelli E., Worrell J. (eds) 48th International Colloquium on Automata, Languages, and Programming (ICALP 2021), Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, 2021. V. 198. № 106. P. 1–19. https://doi.org/10.4230/LIPIcs.ICALP.2021.106
9. *Lagarias J.C., Odlyzko A.M.* Solving low-density subset sum problems // J. ACM. 1985. V. 32. № 1. P. 229–246. https://doi.org/10.1145/2455.2461
10. *Coster M.J., Joux A., LaMacchia B.A., Odlyzko A.M., Schnorr C.P., Stern J.* Improved low-density subset sum algorithms // Comput. Complexity. 1992. V. 2. № 2. P. 111–128. https://doi.org/10.1007/BF01201999
11. *May A.* Solving subset sum with small space – Handling cryptanalytic Big Data // it – Information Technology. 2020. V. 62. № 3–4. P. 181–187. https://doi.org/10.1515/itit-2019-0038
12. *Рыбалов А.Н.* О генерической сложности проблемы о сумме подмножеств для полугрупп целочисленных матриц // Прикладная дискретная математика. 2020. № 50. С. 118–126. https://doi.org/10.17223/20710410/50/9
13. *Кузюрин Н.Н.* Полиномиальный в среднем алгоритм в целочисленном линейном программировании // Сиб. журн. исслед. опер. 1994. Т. 1. № 3. С. 38–48.
14. *Kuzyurin N.N.* An integer linear programming algorithm polynomial in the average case // In: Korshunov A.D. (eds.) Discrete Analysis and Operations Research. Mathematics and Its Applications. V. 355. P. 143–152. Springer, Dordrecht, 1996. https://doi.org/10.1007/978-94-009-1606-7
15. *Селиверстов А.В.* Двоичные решения для больших систем линейных уравнений // Прикладная дискретная математика. 2021. № 52. С. 5–15. https://doi.org/10.17223/20710410/52/1
16. *Pan Y., Zhang F.* Solving low-density multiple subset sum problems with SVP oracle // J. Syst. Sci. Complex. 2016. V. 29. P. 228–242. https://doi.org/10.1007/s11424-015-3324-9

17. *Селиверстов А.В.* О двоичных решениях систем уравнений // Прикладная Дискретная Математика. 2019. № 45. С. 26–32.
https://doi.org/10.17223/20710410/45/3

18. *Martins J.P., Ribas B.C.* A randomized heuristic repair for the multidimensional knapsack problem // Optim. Lett. 2021. V. 15. P. 337–355.
https://doi.org/10.1007/s11590-020-01611-1

19. *Cacchiani V., Iori M., Locatelli A., Martello S.* Knapsack problems – An overview of recent advances. Part II: Multiple, multidimensional, and quadratic knapsack problems // Comput. and Operat. Res. 2022. V. 143. № 105693. P. 1–14.
https://doi.org/10.1016/j.cor.2021.105693

20. *Gribanov D.V., Zolotykh N.Y.* On lattice point counting in Δ-modular polyhedra // Optim. Lett. 2022. V. 16. P. 1991–2018.
https://doi.org/10.1007/s11590-021-01744-x

21. *Al-Shihabi S.* A novel core-based optimization framework for binary integer programs – the multidemand multidimesional knapsack problem as a test problem // Operat. Res. Perspectiv. 2021. V. 8. № 100182. P. 1–13.
https://doi.org/10.1016/j.orp.2021.100182

22. *Лотов А.В., Рябиков А.И.* Дополненный метод стартовой площадки для аппроксимации границы Парето в задачах с многоэкстремальными критериями // Ж. вычисл. матем. и матем. физ. 2021. Т. 61. № 10. С. 1734–1744.
https://doi.org/10.31857/S0044466921100100

23. *Жадан В.Г.* Прямо-двойственный метод Ньютона с наискорейшим спуском для линейной задачи полуопределенного программирования. Ньютоновская система уравнений // Ж. вычисл. матем. и матем. физ. 2022. Т. 62. № 2. С. 232–248.
https://doi.org/10.31857/S0044466922020132

24. *Fu H., Xu Y., Wu G., Liu J., Chen S., He X.* Emphasis on the flipping variable: Towards effective local search for hard random satisfiability // Informat. Sci. 2021. V. 566. P. 118–139.
https://doi.org/10.1016/j.ins.2021.03.009

25. *Fu H., Liu J., Wu G., Xu Y., Sutcliffe G.* Improving probability selection based weights for satisfiability problems // Knowledge-Based Systems. 2022. V. 245. № 108572. P. 1–17.
https://doi.org/10.1016/j.knosys.2022.108572

26. *Guo P., Zhang Y.* ISSATA: An algorithm for solving the 3-satisfiability problem based on improved strategy // Applied Intelligence. 2022. V. 52. P. 1740–1751.
https://doi.org/10.1007/s10489-021-02493-1

27. *Cai S., Lei Z.* Old techniques in new ways: Clause weighting, unit propagation and hybridization for maximum satisfiability // Artificial Intelligence. 2020. V. 287. № 103354. P. 1–14.
https://doi.org/10.1016/j.artint.2020.103354

28. *Li W., Xu C., Yang Y., Chen J., Wang J.* A refined branching algorithm for the maximum satisfiability problem // Algorithmica. 2022. V. 84. P. 982–1006.
https://doi.org/10.1007/s00453-022-00938-8

29. *Абрамов С.А.* Лекции о сложности алгоритмов. М: МЦНМО, 2012.

30. *Алаев П.Е., Селиванов В.Л.* Поля алгебраических чисел, вычислимые за полиномиальное время. I // Алгебра и логика. 2019. Т. 58, № 6. С. 673–705.
https://doi.org/10.33048/alglog.2019.58.601

31. *Батхин А.Б.* Параметризация дискриминантного множества многочлена // Программирование. 2016. № 2. С. 8–21.

32. *Селиверстов А.В.* Эвристические алгоритмы распознавания некоторых кубических гиперповерхностей // Программирование. 2021. № 1. С. 65–72.
https://doi.org/10.31857/S0132347421010106

33. *Schwartz J.* Fast probabilistic algorithms for verification of polynomial identities // J. ACM. 1980. V. 27. № 4. P. 701–717.
https://doi.org/10.1145/322217.322225

34. *Halbeisen L., Hungerbühler N., Schumacher S.* Magic sets for polynomials of degree *n* // Linear Algebra Appl. 2021. V. 609. P. 413–441.
https://doi.org/10.1016/j.laa.2020.09.026

35. *Chistov A.L.* Fast parallel calculation of the rank of matrices over a field of arbitrary characteristic // In: L. Budach (eds) Fundamentals of Computation Theory. FCT 1985. Lecture Notes in Computer Science, vol. 199. Springer, Berlin, Heidelberg, 1985. P. 63–69.
https://doi.org/10.1007/BFb0028792

36. *Mulmuley K.* A fast parallel algorithm to compute the rank of a matrix over an arbitrary field // Combinatorica. 1987. V. 7. № 1. P. 101–104.
https://doi.org/10.1007/BF02579205

37. *Переславцева О.Н.* О вычислении характеристического полинома матрицы // Дискретная матем. 2011. Т. 23. № 1. С. 28–45.
https://doi.org/10.4213/dm1128

38. *Cheung H.Y., Kwok T.C., Lau L.C.* Fast matrix rank algorithms and applications // J. ACM. 2013. V. 60. № 5. Article № 31. P. 1–25.
https://doi.org/10.1145/2528404

39. *Malaschonok G.I., Seliverstov A.V.* Calculation of integrals in MathPartner // Discrete and Continuous Model. and Appl. Comput. Sci. 2021. V. 29. № 4. P. 337–346.
https://doi.org/10.22363/2658-4670-2021-29-4-337-346

40. *Seliverstov A.V., Lyubetsky V.A.* About forms equal to zero at each vertex of a cube // J. of Communicat. Techn. and Electron. 2012. V. 57. № 8. P. 892–895.
https://doi.org/10.1134/S1064226912080049