ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.161

ДВОИЧНЫЕ РЕШЕНИЯ ДЛЯ БОЛЬШИХ СИСТЕМ ЛИНЕЙНЫХ УРАВНЕНИЙ[1]

А. В. Селиверстов

Институт проблем передачи информации им. А. А. Харкевича Российской академии наук, г. Москва, Россия

Понятие генерической вычислительной сложности распространено на обобщённые регистровые машины над упорядоченным полем. В этом случае машина на каждом входе останавливается и почти на каждом входе даёт содержательный ответ, но может отказаться от вычисления посредством явного уведомления об этом, иными словами, существует особое неопределённое состояние остановки. При этом машина не делает ошибок. Предложен генерический алгоритм полиномиального времени для распознавания систем линейных уравнений без какого-либо двоичного решения, когда число уравнений m близко к числу неизвестных n. Более точно — требуется выполнение двух условий. Во-первых, выполнено неравенство $2n \geqslant (n-m+1)(n-m+2)$. Такие системы называются большими, поскольку число уравнений близко к числу неизвестных. Во-вторых, выполнены некоторые предположения общности системы уравнений. Наш подход основан на поиске положительно определённой квадратичной формы среди множества форм, зависящих от параметров. С другой стороны, найден контрпример, показывающий неприменимость этого метода для проверки отсутствия двоичного решения у одного уравнения.

Ключевые слова: *двоичное решение, линейное уравнение, обобщённая регистровая машина, вычислительная сложность.*

DOI 10.17223/20710410/52/1

BINARY SOLUTIONS TO LARGE SYSTEMS OF LINEAR EQUATIONS

A. V. Seliverstov

Institute for Information Transmission Problems of the Russian Academy of Sciences (Kharkevich Institute), Moscow, Russia

E-mail: slvstv@iitp.ru

The concept of generic computational complexity has been extended to generalized register machines over an ordered field. In this case, the machine halts at every input and gives a meaningful answer at almost every input, but it can abandon the calculation using explicit notification, that is, there exists the vague halting state. Note that the machine does not make any error. A generic polynomial time algorithm is

[1]Исследование выполнено при финансовой поддержке РФФИ, проект № 18-29-13037.

proposed to recognize systems of linear equations without any binary solution, when the number of equations m is close to the number of unknowns n. More precisely, two conditions are required. Firstly, the inequality $2n \geqslant (n-m+1)(n-m+2)$ holds. Such systems are called large because the number of equations is close to the number of unknowns. Secondly, some assumptions of generality of the system of equations are fulfilled. Our approach is based on finding a positive definite quadratic form among the set of forms that depend on parameters. On the other hand, a counterexample has been found, whicht shows the inapplicability of this method for checking the absence of any binary solution to one equation.

Keywords: *binary solution, linear equation, generalized register machine, computational complexity.*

Введение

Задача о существовании двоичного решения у системы линейных уравнений с рациональными коэффициентами NP-полная [1, следствие 18.1b, т. 2, с. 397], она сводится за полиномиальное время к задаче о существовании двоичного решения одного линейного уравнения. Иногда получается уравнение с целыми коэффициентами, близкими к нулю [2]. Если линейное уравнение имеет целые коэффициенты, чьи модули достаточно малы, то поиск двоичного решения для этого уравнения быстро выполняется методом динамического программирования [1, 3–5]. В случае отсутствия ограничений на коэффициенты для поиска двоичного решения одного линейного уравнения от n неизвестных предложены детерминированный алгоритм, использующий экспоненциальное время $\mathrm{poly}(n)2^{0{,}5n}$ и экспоненциальную память $\mathrm{poly}(n)2^{0{,}25n}$, а также вероятностный алгоритм, использующий большее время $\mathrm{poly}(n)2^{0{,}86n}$, но полиномиальную память [6, 7]. Гипотеза о высокой вычислительной сложности этой задачи согласуется с оценками степеней многочленов, необходимых для доказательства отсутствия двоичного решения посредством Positivstellensatz [8]. Для близкой задачи Equal-Subset-Sum, которая эквивалентна поиску $(-1, 0, 1)$-решения линейного уравнения, известны детерминированный алгоритм с временем работы $\mathrm{poly}(n)3^{0{,}5n}$, а также вероятностный алгоритм, дающий ответ за время $\mathrm{poly}(n)1{,}7088^n$ с высокой вероятностью [9].

Посредством исключения переменных поиск двоичного решения системы из m линейно независимых линейных уравнений от n неизвестных сводится к параллельной проверке продолжаемости двоичных решений одного линейного уравнения от $(n-m)$ неизвестных до двоичного решения системы уравнений от n неизвестных. Следовательно, исходная задача разрешима за полиномиальное время, когда разность между числом неизвестных и числом линейно независимых уравнений ограничена функцией вида $n - m = O(\log n)$. В этой работе мы рассмотрим случай, когда разность числа неизвестных n и числа уравнений m ограничена сверху сравнительно быстро растущей функцией вида $n - m = O(\sqrt{n})$ и выполнено некоторое предположение общности для системы уравнений. Так улучшены ранее полученные оценки, но предложенный метод в общем случае бесполезен для одного уравнения.

Для многих NP-полных задач также известны эвристические алгоритмы, работающие при дополнительных ограничениях. Например, для задачи 3-SAT о выполнимости 3-КНФ при дополнительном условии, когда число элементарных дизъюнкций в 3-КНФ от n переменных ограничено снизу функцией вида $\mathrm{poly}(\log n)n\sqrt{n}$, существует алгоритм полиномиального времени, который для большой доли случаев (при любом фиксированном значении n) распознаёт невыполнимость 3-КНФ [10, 11].

Более сильный результат известен для задачи NAE-3-SAT. Здесь проверяется существование оценки n булевых переменных, при которой каждая элементарная дизъюнкция в 3-КНФ содержит как истинный, так и ложный литералы. При дополнительном условии, когда число элементарных дизъюнкций в 3-КНФ превышает $\frac{27}{2}n$, существует алгоритм полиномиального времени, который для большой доли случаев (при любом фиксированном значении n), стремящейся к единице с ростом n, распознаёт отсутствие решения [12].

1. Вычислительная модель

Оценивая вычислительную сложность, мы рассматриваем обобщённые регистровые машины над упорядоченным полем $(K, 0, 1, +, -, \times, ()^{-1}, <, =)$, которое вложено в поле вещественных чисел [13]. Над полем вещественных чисел такая модель вычислений известна как BSS-машина [14]. Элементы поля K будем называть числами, но можно рассматривать любые упорядоченные поля. Здесь $x^{-1}x = 1$, когда $x \neq 0$, и дополнительно $0^{-1} = 0$. Каждый регистр содержит число из поля K. Машина имеет также индексные регистры, содержащие неотрицательные целые числа. За один шаг машина либо выполняет операцию над индексными регистрами, либо копирует число из одного регистра в другой, либо записывает в регистр константу 0 или 1, либо вычисляет сумму, разность или произведение двух чисел в регистрах, либо вычисляет обратное число к записанному в регистр, либо выполняет сравнение двух чисел в регистрах. При этом номера используемых регистров хранятся в индексных регистрах, над которыми производятся обычные операции. Время работы полиномиальное, если общее число операций, выполняемых машиной до остановки, ограничено многочленом от числа регистров, занятых входом. В начальный момент времени это число записано в нулевом индексном регистре, а другие индексные регистры содержат нули. Так же определяются недетерминированные обобщённые регистровые машины. Недетерминированный шаг состоит в записи в указанный регистр нового числа из поля K, которое не было вычислено на предыдущих шагах.

Говоря менее формально, рассматривая обобщённые регистровые машины, мы оцениваем арифметическую сложность. С другой стороны, вычисления на обобщённых регистровых машинах тесно связаны с методами алгебраической геометрии над произвольными алгебраическими структурами [15]. Над полем, вычислимым за полиномиальное время, полиномиальная вычислимость на обобщённой регистровой машине не влечёт полиномиально ограниченную битовую сложность [16, 17]. Для этого дополнительно требуется, чтобы на каждом шаге записанные в регистрах числа имели полиномиально ограниченную длину записи. Это ограничение существенно. Например, возведение рационального числа в степень n требует лишь $O(\log n)$ умножений. Однако в общем случае длина двоичной записи результата не ограничена сверху функцией типа $\mathrm{poly}(\log n)$. С другой стороны, трудно указать минимальное число умножений, необходимое для вычисления такого числа оптимальным способом [18].

Для положительного целого числа k фраза «почти все последовательности из k чисел» обозначает «все численные оценки k переменных, на которых как-то фиксированный многочлен положительной степени от k переменных не обращается в нуль» [19]. Многочлен отождествляется с последовательностью числовых коэффициентов, включая нулевые значения, используя фиксированное мономиальное упорядочение. Так же с последовательностями чисел отождествляются системы уравнений и матрицы, чьи элементы упорядочиваются в зависимости от контекста.

Мы рассматриваем машины, которые могут давать неопределённый результат — отказ от вычисления. Но принимая или отвергая вход, машина не ошибается. Рассмотрим обобщённую регистровую машину над упорядоченным полем с тремя состояниями остановки, обозначаемыми через ACCEPT, REJECT и VAGUE. В состоянии ACCEPT машина принимает вход, в состоянии REJECT — отвергает вход, в состоянии VAGUE — отказывается дать содержательный ответ. По аналогии с обычными генерическими вычислениями [20–23] обобщённая регистровая машина называется *генерической*, когда выполнены два условия: 1) машина останавливается на каждом входе и 2) для каждого положительного целого числа k и для почти всех входов, каждый из которых занимает ровно k регистров, машина принимает или отвергает вход, но не останавливается в состоянии VAGUE. Аналогично определяются генерические машины, вычисляющие нетривиальный выход в регистрах. Если машина остановилась в состоянии VAGUE, то записанный в регистрах выход признаётся бессмысленным. Однако для любого k и для почти всех входов, каждый из которых занимает ровно k регистров, машина не приходит в состояние VAGUE.

Над полем вещественных чисел множество входов, на котором генерическая обобщённая регистровая машина останавливается в состоянии VAGUE, имеет меру нуль. Поэтому такие машины служат аналогом обычных генерических алгоритмов.

Часто условием вычислимости служит ограничение на ранг матрицы. В общем случае степень детерминатального многообразия (над полем комплексных чисел) может очень быстро расти при увеличении размера (прямоугольной) матрицы [24]. Однако над линейно упорядоченным полем верхняя граница k на ранг матрицы выражается обращением в нуль суммы квадратов миноров порядка k. Это многочлен степени $2k$ от элементов матрицы.

Для чисел n и $r \leqslant n$ ранг $(r \times n)$-матрицы равен r тогда и только тогда, когда отличен от нуля некоторый многочлен степени $2r$ от элементов матрицы. При этом достаточным условием, которое выполнено для почти всех таких матриц, служит отличие от нуля одного из миноров порядка r, равного многочлену степени r.

Согласно критерию Сильвестра, симметричная матрица положительно определена тогда и только тогда, когда все её угловые миноры Δ_k положительные. Определитель матрицы над полем K вычисляется обобщённой регистровой машиной за полиномиальное время. Для проверки положительной определённости числовой матрицы удобно использовать также LDU-разложение, чья вычислительная сложность имеет тот же порядок, что и для матричного умножения [25].

2. Основные результаты

Для каждого натурального числа n рассмотрим n-мерное аффинное пространство над полем K с фиксированной системой координат. Точка, каждая координата которой равна 0 или 1, называется $(0,1)$-точкой. Поиск бинарного решения системы линейных уравнений эквивалентен поиску $(0,1)$-точки, инцидентной аффинному подпространству. Многочлен второй степени, который равен линейной комбинации многочленов вида $x_k(x_k-1)$, обращается в нуль в каждой $(0,1)$-точке. Гомогенизацией такого многочлена служит линейная комбинация квадратичных форм вида $x_k(x_k-x_0)$, где через x_0 обозначена новая переменная. Такие квадратичные формы служат для сертификации отсутствия двоичных решений.

Аффинное пространство вложено в проективное пространство с однородными координатами $(x_0 : \cdots : x_n)$. При $\alpha \neq 0$ линейная форма αx_0 определяет бесконечно

удалённую гиперплоскость в проективном пространстве. Аффинное пространство соответствует значению $x_0 = 1$.

Теорема 1. Даны натуральные числа n и s, для которых выполнено неравенство $2n \geqslant (s+1)(s+2)$. Для почти каждого набора из $(n-s)$ линейных форм $\ell_j(x_0, \cdots, x_s)$ для индексов $j > s$ найдутся такие значения коэффициентов λ_k, что будет положительно определена квадратичная форма

$$\sum_{k=1}^{s} \lambda_k x_k(x_k - x_0) + \sum_{j=s+1}^{n} \lambda_j \ell_j(\ell_j - x_0)$$

от переменных x_0, …, x_{n-s}. Более того, значения этих коэффициентов вычисляются генерической обобщённой регистровой машиной за полиномиальное время. Эта машина может остановиться в состоянии VAGUE лишь на таком входе, на котором обращается в нуль некоторый многочлен степени не выше $(s+1)(s+2)$ от коэффициентов линейных форм ℓ_j.

Доказательство. Достаточно найти значения λ_1, …, λ_n, при которых выполнено равенство многочленов

$$\sum_{k=1}^{s} \lambda_k x_k(x_k - x_0) + \sum_{j=s+1}^{n} \lambda_j \ell_j(\ell_j - x_0) = \sum_{k=0}^{s} x_k^2.$$

Этот набор значений служит решением неоднородной системы линейных уравнений от n неизвестных $\lambda_1, \ldots, \lambda_n$, в которой число уравнений равно $s+1$. Обозначим через ℓ_{jk} коэффициенты линейной формы $\ell_j = \ell_{j0}x_0 + \ldots + \ell_{js}x_s$. Коэффициенты при мономах x_0^2 определяют для неизвестных λ_1, …, λ_n неоднородное уравнение

$$\sum_{j=s+1}^{n} \ell_{j0}(\ell_{j0} - 1)\lambda_j = 1. \tag{1}$$

Коэффициенты при мономах x_k^2, где $1 \leqslant k \leqslant s$, дают s уравнений

$$\lambda_k + \sum_{j=s+1}^{n} \ell_{jk}^2 \lambda_j = 1. \tag{2}$$

Коэффициенты при мономах $x_k x_0$, где $1 \leqslant k \leqslant s$, дают s уравнений

$$-\lambda_k + \sum_{j=s+1}^{n} \ell_{jk}(2\ell_{j0} - 1)\lambda_j = 0. \tag{3}$$

Коэффициенты при мономах $x_k x_i$, где $1 \leqslant i < k \leqslant s$, дают уравнения

$$\sum_{j=s+1}^{n} \ell_{jk}\ell_{ji}\lambda_j = 0. \tag{4}$$

Обозначим через r число уравнений от неизвестных λ_1, …, λ_n, которое составляет $r = \dfrac{1}{2}(s+1)(s+2) \leqslant n$. Достаточным условием существования решения служит полный ранг матрицы такой системы. Для этого достаточно отличия от нуля одного из миноров Δ_r порядка r этой $(r \times n)$-матрицы, который служит многочленом степени r от элементов матрицы. Элемент матрицы — это (вообще говоря, неоднородный) многочлен степени не выше второй от коэффициентов линейных форм ℓ_j. Следовательно,

минор Δ_r — это многочлен от коэффициентов линейных форм ℓ_j, степень которого не превышает $2r = (s+1)(s+2)$. Для завершения доказательства нужно показать, что этот многочлен не равен нулю тождественно.

Обозначим через $c(i,k)$ номер пары индексов (i,k), $1 \leqslant i \leqslant k \leqslant s$, принимающий значения от 1 до $r-s-1$. Рассмотрим набор линейных форм $\ell_j = \frac{1}{2}x_0 + x_i + x_k$, где при $s+1 \leqslant j \leqslant r-1$ индексы связаны уравнением $j = s + c(i,k)$. При $j = r$ полагаем $\ell_r = \frac{1}{2}x_0$. При $j > r$ полагаем $\ell_j = 0$.

Уравнение (1) принимает вид $-\frac{1}{4}(\lambda_{s+1} + \ldots + \lambda_r) = 1$. Уравнения типа (2) принимают вид $\lambda_k + 4\lambda_j = 1$, где $1 \leqslant k \leqslant s$ и $j = s + c(k,k)$. Уравнения типа (3) принимают вид $-\lambda_k = 0$, где $1 \leqslant k \leqslant s$. Складывая соответствующие уравнения типов (2) и (3), получим уравнения типа $4\lambda_j = 1$, где $1 \leqslant k \leqslant s$ и $j = s + c(k,k)$. Уравнения типа (4) принимают вид $\lambda_j = 0$, где $1 \leqslant i < k \leqslant s$ и $j = s + c(i,k)$.

Итак, при выбранных линейных формах ℓ_j подсистема без уравнения (1) эквивалентна системе уравнений, каждое из которых зависит от одной из переменных λ_1, $\ldots$, λ_{r-1} без повторений. Число этих уравнений равно $r-1$. Следовательно, эта система имеет единственное решение. Также существует единственное значение λ_r, при котором это решение продолжается до решения уравнения (1). При $n > r$ значения λ_{r+1}, $\ldots$, λ_n могут быть любыми. Поэтому соответствующая матрица имеет полный ранг r, а её угловой минор Δ_r отличен от нуля. ■

Замечание 1. Над полем рациональных чисел $\mathbb{Q}$ битовая вычислительная сложность поиска коэффициентов λ_1, $\ldots$, λ_n также полиномиально ограничена, поскольку задача сводится к решению системы линейных уравнений. При этом суммарный размер двоичных записей чисел на промежуточных шагах вычисления ограничен многочленом от длины входа [1, теорема 3.3, т. 1, с. 55]. Более того, так получается генерический алгоритм полиномиального времени в смысле определения из работ [20–23]. Если на вход поступают рациональные числа, чьи длины двоичных записей ограничены сверху многочленом $\mathrm{poly}(n)$, то верхняя оценка доли тех входов, на которых машина останавливается в состоянии VAGUE, получается из леммы Шварца — Зиппеля [26].

Теорема 2. Для любых натуральных чисел n и s, удовлетворяющих неравенству $2n \geqslant (s+1)(s+2)$, и для почти каждого набора $(n-s)$ линейных форм $\ell_j(x_0, \cdots, x_s)$ для индексов $j > s$ генерическая обобщённая регистровая машина за полиномиальное время распознаёт отсутствие какой-либо $(0,1)$-точки, инцидентной аффинному подпространству, заданному системой уравнений $x_j = \ell_j(1, x_1, \cdots, x_s)$ для индексов $j > s$. Более того, эта машина может остановиться в состоянии VAGUE лишь на таком входе, на котором обращается в нуль некоторый многочлен степени не выше $(s+1)(s+2)$ от коэффициентов линейных форм ℓ_j.

Доказательство. Согласно теореме 1, генерическая обобщённая регистровая машина за полиномиальное время вычисляет такие коэффициенты λ_1, $\ldots$, λ_n, что при значении переменной $x_0 = 1$ выполнено равенство

$$\sum_{k=1}^{s} \lambda_k x_k(x_k - 1) + \sum_{j=s+1}^{n} \lambda_j \ell_j(\ell_j - 1) = 1 + \sum_{k=1}^{s} x_k^2.$$

Этот многочлен нигде не обращается в нуль. Однако он должен обращаться в нуль в каждой $(0,1)$-точке, принадлежащей аффинному подпространству, определяемому

системой уравнений $x_j = \ell_j(1, x_1, \ldots, x_s)$ для индексов $j > s$. Следовательно, такой ответ служит подтверждением, что никакая $(0,1)$-точка не принадлежит этому аффинному подпространству. Иначе машина останавливается в состоянии VAGUE. Оценка степени многочлена, обращающегося при этом в нуль, совпадает с оценкой из теоремы 1. ■

Теорема 3. Существует такое число $\varepsilon > 0$, что для любых чисел α и γ из интервала $(1-\varepsilon, 1+\varepsilon)$ и для любых чисел β, λ_1, λ_2 и λ_3 квадратичная форма от трёх переменных x_0, x_1 и x_2, равная

$$\lambda_1 x_1(x_1 - x_0) + \lambda_2 x_2(x_2 - x_0) + \lambda_3 \left(\alpha x_1 + \beta x_2 - \frac{1}{2}\gamma x_0\right)\left(\alpha x_1 + \beta x_2 - \frac{1}{2}\gamma x_0 - x_0\right),$$

не бывает положительно определена.

Доказательство. При $\alpha = \beta = \gamma = 1$ матрица Гессе квадратичной формы равна

$$\begin{pmatrix} \frac{3}{2}\lambda_3 & -\lambda_1 - 2\lambda_3 & -\lambda_2 - 2\lambda_3 \\ -\lambda_1 - 2\lambda_3 & 2\lambda_1 + 2\lambda_3 & 2\lambda_3 \\ -\lambda_2 - 2\lambda_3 & 2\lambda_3 & 2\lambda_2 + 2\lambda_3 \end{pmatrix}.$$

Её угловой минор второго порядка $\Delta_2 = -\lambda_1\lambda_3 - \lambda_1^2 - \lambda_3^2$ не принимает положительных значений. В общем случае

$$\Delta_2 = \lambda_1(\lambda_3\alpha)\left(\frac{\gamma}{\alpha}(\gamma+2) - 2\gamma - 2\right) - \lambda_1^2 - (\lambda_3\alpha)^2.$$

При малых значениях ε выполнены неравенства

$$-2 < \left(\frac{\gamma}{\alpha}(\gamma+2) - 2\gamma - 2\right) < 0.$$

Поэтому угловой минор второго порядка не принимает положительных значений. Следовательно, эта матрица Гессе (и соответствующая квадратичная форма) не бывает положительно определена ни при каких значениях коэффициентов λ_1, λ_2 и λ_3. ■

3. Обсуждение

Теоремы 1 и 3 имеют ясный геометрический смысл над полем вещественных чисел. Однородные координаты в проективном пространстве нигде не обращаются в нуль одновременно. Следовательно, положительно определённая квадратичная форма задаёт в проективном пространстве алгебраическое множество без вещественных точек — мнимый эллипсоид. Если же квадратичная форма не является знакоопределённой, то она обращается в нуль в некоторой вещественной точке проективного пространства. Эта точка может быть бесконечно удалённой, то есть не принадлежать аффинному пространству.

При $n = 3$ и $s = 1$ из теоремы 1 следует, что прямая общего положения в $\mathbb{R}^3$ не пересекает некоторую поверхность второго порядка, проходящую через все $(0,1)$-точки. Это выполнено и для проективного замыкания.

Согласно теореме 3, каждая проективная плоскость в $\mathbb{RP}^3$, заданная уравнением $x_3 = \alpha x_1 + \beta x_2 - \frac{1}{2}\gamma x_0$, где $\alpha \approx 1$ и $\gamma \approx 1$, пересекает в вещественных точках каждую поверхность второго порядка, проходящую через все $(0,1)$-точки аффинного пространства, в котором $x_0 = 1$. Такие плоскости соответствуют непустому открытому

(в аналитической топологии) множеству в пространстве параметров. Следовательно, условие $2n \geqslant (s+1)(s+2)$ в теореме 1 нельзя ослабить при $n = 3$.

Проверяемое генерическим алгоритмом в доказательстве теоремы 1 достаточное условие можно ослабить, если не требовать быстрой вычислимости искомых коэффициентов $\lambda_1, \ldots, \lambda_n$. С другой стороны, если не вычислять, а недетерминированно угадать эти коэффициенты, то за полиномиальное время можно проверить, будет ли полученная квадратичная форма положительно определена. Поэтому меньше отказов от вычисления может обеспечить недетерминированная обобщённая регистровая машина над упорядоченным полем. Однако теорема 3 показывает, что и в этом случае отсутствие решения $\lambda_1, \ldots, \lambda_n$ не означает отсутствия $(0,1)$-точки, принадлежащей данному подпространству.

Детерминированный генерический алгоритм в теореме 2 либо корректно распознаёт отсутствие двоичного решения у большой системы уравнений, либо даёт неопределённый ответ. С другой стороны, двоичное решение можно искать бинарным поиском, проверяя этим алгоритмом отсутствие двоичных решений при оценках некоторых переменных. Например, если при некоторой $(0,1)$-оценке одной из переменных система не имеет двоичного решения, то число неизвестных уменьшается. Однако при неопределённом ответе требуется проверка новых гипотез. Поэтому в худшем случае требуется перебор большого числа гипотез даже для систем, включающих много линейно независимых уравнений. Теорема 2 не позволила также улучшить результаты о выполнимости 3-КНФ. Хотя обе задачи 3-SAT и NAE-3-SAT сводятся к поиску двоичных решений у системы линейных уравнений, в интересных случаях число линейно независимых уравнений оказывается значительно меньше числа переменных.

Алгоритм в теореме 2 нельзя применить для проверки существования двоичного решения у одного линейного уравнения. Теорема 3 подтверждает это при $n = 3$.

Заключение

Понятие генерического алгоритма распространено на обобщённые регистровые машины над упорядоченным полем. Предложен генерический алгоритм полиномиального времени для распознавания систем линейных уравнений без какого-либо двоичного решения, когда число уравнений m и число неизвестных n связаны неравенством $2n \geqslant (n-m+1)(n-m+2)$. Этот алгоритм распознавания служит для обоснования эвристического метода поиска двоичного решения такой системы уравнений. Однако в худшем случае поиск двоичного решения остаётся вычислительно трудной задачей.

ЛИТЕРАТУРА

1. *Схрейвер А.* Теория линейного и целочисленного программирования. В 2-х т.М.: Мир, 1991. 702 с.
2. *Селиверстов А. В.* О двоичных решениях систем уравнений // Прикладная дискретная математика. 2019. № 45. С. 26–32.
3. *Koiliaris K. and Xu C.* Faster pseudopolynomial time algorithms for subset sum // ACM Trans. Comput. Theory. 2019. V. 15. No. 3. Article 40.
4. *Curtis V. V., Sanches C. A. A.* An improved balanced algorithm for the subset-sum problem // European J. Operational Res. 2019. V. 275. P. 460–466.
5. *Mucha M., Węgrzycki K., and Włodarczyk M.* A subquadratic approximation scheme for partition // Proc. Ann. ACM-SIAM Symp. Discrete Algorithms. Philadelphia: SIAM, 2019. P. 70–88.

6. *Schroeppel R. and Shamir A.* A $T = O(2^{n/2})$, $S = O(2^{n/4})$ algorithm for certain NP-complete problems // SIAM J. Computing. 1981. V. 10. No. 3. P. 456–464.
7. *Bansal N., Garg S., Nederlof J., and Vyas N.* Faster space-efficient algorithms for subset sum, k-sum, and related problems // SIAM J. Computing. 2018. V. 47. No. 5. P. 1755–1777.
8. *Grigoriev D.* Complexity of Positivstellensatz proofs for the knapsack // Comput. Complexity. 2001. V. 10. P. 139–154.
9. *Mucha M., Nederlof J., Pawlewicz J., and Węgrzycki K.* Equal-subset-sum faster than the meet-in-the-middle // 27th Ann. Europ. Symp. Algorithms, ESA 2019. Leibniz Intern. Proc. Informatics, LIPIcs. V. 144. Schloss Dagstuhl, Leibniz-Zentrum für Informatik, 2019. Article 73.
10. *Goerdt A. and Lanka A.* Recognizing more random unsatisfiable 3-SAT instances efficiently // Electronic Notes in Discrete Math. 2003. V. 16. P. 21–46.
11. *Brown-Cohen J. and Raghavendra P.* Extended formulation lower bounds for refuting random CSPs // Proc. ACM-SIAM Symp. Discrete Algorithms. Philadelphia: SIAM, 2020. P. 305–324.
12. *Deshpande Y., Montanari A., O'Donnell R., et al.* The threshold for SDP-refutation of random regular NAE-3SAT // Proc. Ann. ACM-SIAM Symp. Discrete Algorithms. Philadelphia: SIAM, 2019. P. 2305–2321.
13. *Neumann E. and Pauly A.* A topological view on algebraic computation models // J. Complexity. 2018. V. 44. P. 1–22.
14. *Blum L., Shub M., and Smale S.* On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines // Bull. American Mathematical Society (N.S.). 1989. V. 21. No. 1. P. 1–46.
15. *Даниярова Э. Ю., Мясников А. Г., Ремесленников В. Н.* Алгебраическая геометрия над алгебраическими системами. IX. Главные универсальные классы и Dis-пределы // Алгебра и логика. 2018. Т. 57. № 6. С. 639–661.
16. *Алаев П. Е., Селиванов В. Л.* Поля алгебраических чисел, вычислимые за полиномиальное время. I // Алгебра и логика. 2019. Т. 58. № 6. С. 673–705.
17. *Алаев П. Е.* Полиномиально вычислимые структуры с конечным числом порождающих // Алгебра и логика. 2020. Т. 59. № 3. С. 385–394.
18. *Коточигов А. М., Сучков А. И.* Метод сокращения перебора в алгоритмах построения минимальных аддитивных цепочек // Компьютерные инструменты в образовании. 2020. № 1. С. 5–18.
19. *Селиверстов А. В.* Симметричные матрицы, элементами которых служат линейные функции // Журн. вычислительной математики и математической физики. 2020. Т. 60. № 1. С. 109–115.
20. *Рыбалов А. Н.* О генерической неразрешимости десятой проблемы Гильберта для полиномиальных деревьев // Прикладная дискретная математика. 2019. № 44. С. 107–112.
21. *Рыбалов А. Н.* О генерической NP-полноте проблемы выполнимости булевых схем // Прикладная дискретная математика. 2020. № 47. С. 101–107.
22. *Рыбалов А. Н.* О генерической сложности проблемы представимости натуральных чисел суммой двух квадратов // Прикладная дискретная математика. 2020. № 48. С. 93–99.
23. *Рыбалов А. Н.* О генерической сложности экзистенциальных теорий // Прикладная дискретная математика. 2020. № 49. С. 120–126.
24. *Harris J. and Tu L. W.* On symmetric and skew-symmetric determinantal varieties // Topology. 1984. V. 23. No. 1. P. 71–84.
25. *Malaschonok G. and Scherbinin A.* Triangular decomposition of matrices in a domain // LNCS. 2015. V. 9301. P. 292–306.

26. *Schwartz J. T.* Fast probabilistic algorithms for verification of polynomial identities // J. ACM. 1980. V. 27. No. 4. P. 701–717.

REFERENCES

1. *Schrijver A.* Theory of linear and integer programming. New York, John Wiley & Sons, 1986.
2. *Seliverstov A. V.* O dvoichnykh resheniyakh sistem uravneniy [On binary solutions to system of equations]. Prikladnaya Diskretnaya Matematika, 2019, no. 45, pp. 26–32. (in Russian)
3. *Koiliaris K. and Xu C.* Faster pseudopolynomial time algorithms for subset sum. ACM Trans. Comput. Theory, 2019, vol. 15, no. 3, article 40.
4. *Curtis V. V. and Sanches C. A. A.* An improved balanced algorithm for the subset-sum problem. European J. Operational Res., 2019, vol. 275, pp. 460–466.
5. *Mucha M., Węgrzycki K., and Włodarczyk M.* A subquadratic approximation scheme for partition. Proc. Ann. ACM-SIAM Symp. Discrete Algorithms, 2019, pp. 70–88.
6. *Schroeppel R. and Shamir A.* A $T = O(2^{n/2})$, $S = O(2^{n/4})$ algorithm for certain NP-complete problems. SIAM J. Computing, 1981, vol. 10, no. 3, pp. 456–464.
7. *Bansal N., Garg S., Nederlof J., and Vyas N.* Faster space-efficient algorithms for subset sum, k-sum, and related problems. SIAM J. Computing, 2018, vol. 47, no. 5, pp. 1755–1777.
8. *Grigoriev D.* Complexity of Positivstellensatz proofs for the knapsack. Comput. Complexity, 2001, vol. 10, pp. 139–154.
9. *Mucha M., Nederlof J., Pawlewicz J., and Węgrzycki K.* Equal-subset-sum faster than the meet-in-the-middle. 27th Ann. European Symp. Algorithms, ESA 2019. Leibniz Intern. Proc. Informatics, LIPIcs, vol. 144, Schloss Dagstuhl, Leibniz-Zentrum für Informatik, 2019. Article 73.
10. *Goerdt A. and Lanka A.* Recognizing more random unsatisfiable 3-SAT instances efficiently. Electronic Notes in Discrete Math., 2003, vol. 16, pp. 21–46.
11. *Brown-Cohen J. and Raghavendra P.* Extended formulation lower bounds for refuting random CSPs. Proc. ACM-SIAM Symp. Discrete Algorithms, 2020, pp. 305–324.
12. *Deshpande Y., Montanari A., O'Donnell R., et al.* The threshold for SDP-refutation of random regular NAE-3SAT. Proc. Ann. ACM-SIAM Symp. Discrete Algorithms, 2019, pp. 2305–2321.
13. *Neumann E. and Pauly A.* A topological view on algebraic computation models. J. Complexity, 2018, vol. 44, pp. 1–22.
14. *Blum L., Shub M., and Smale S.* On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. Bull. American Mathematical Society (N.S.), 1989, vol. 21, no. 1, pp. 1–46.
15. *Daniyarova E. Yu., Myasnikov A. G., and Remeslennikov V. N.* Algebraic geometry over algebraic structures. IX. Principal universal classes and Dis-limits. Algebra and Logic, 2019, vol. 57, no. 6, pp. 414–428.
16. *Alaev P. E. and Selivanov V. L.* Fields of algebraic numbers computable in polynomial time. I. Algebra and Logic, 2020, vol. 58, no. 6, pp. 447–469.
17. *Alaev P. E.* Polynomially computable structures with finitely many generators. Algebra and Logic, 2020, vol. 59, no. 3, pp. 266–272.
18. *Kotochigov A. M. and Suchkov A. I.* Metod sokrashcheniya perebora v algoritmakh postroeniya minimal'nykh additivnykh tsepochek [A method for reducing iteration in algorithms for building minimal additive chains]. Komp'yuternye Instrumenty v Obrazovanii, 2020, no. 1, pp. 5–18. (in Russian).
19. *Seliverstov A. V.* Symmetric matrices whose entries are linear functions. Comput. Math. and Math. Physics, 2020, vol. 60, no. 1, pp. 102–108.

20. *Rybalov A. N.* O genericheskoy nerazreshimosti desyatoy problemy Gil'berta dlya polinomial'nykh derev'ev [On generic undecidability of Hilbert's tenth problem for polynomial trees]. Prikladnaya Diskretnaya Matematika, 2019, no. 44, pp. 107–112. (in Russian).
21. *Rybalov A. N.* O genericheskoy NP-polnote problemy vypolnimosti bulevykh skhem [On generic NP-completeness of the problem of Boolean circuits satisfiability]. Prikladnaya Diskretnaya Matematika, 2020, no. 47, pp. 101–107. (in Russian).
22. *Rybalov A. N.* O genericheskoy slozhnosti problemy predstavimosti natural'nykh chisel summoy dvukh kvadratov [On generic complexity of the problem of representation of natural numbers by sum of two squares]. Prikladnaya Diskretnaya Matematika, 2020, no. 48, pp. 93–99. (in Russian).
23. *Rybalov A. N.* O genericheskoy slozhnosti ekzistentsial'nykh teoriy [On generic complexity of the existential theories]. Prikladnaya Diskretnaya Matematika, 2020, no. 49, pp. 120–126. (in Russian).
24. *Harris J. and Tu L. W.* On symmetric and skew-symmetric determinantal varieties. Topology, 1984, vol. 23, no. 1, pp. 71–84.
25. *Malaschonok G. and Scherbinin A.* Triangular decomposition of matrices in a domain. LNCS, 2015, vol. 9301, pp. 292–306.
26. *Schwartz J. T.* Fast probabilistic algorithms for verification of polynomial identities. J. ACM, 1980, vol. 27, no. 4, pp. 701–717.