УДК 512.644
AMS MSC2020: 15A06

О сводимости систем линейных уравнений

Селиверстов А. В.

Институт проблем передачи информации им. А. А. Харкевича РАН

Аннотация. Рассмотрена задача распознавания, существует ли $(0,1)$-решение для системы линейных уравнений с целыми коэффициентами. Алгебраический подход позволяет уточнить структуру множества трудных входов. С другой стороны, количество $(0,1)$-решений одного линейного уравнения от n переменных равно количеству $(0,1)$-решений системы линейных уравнений, коэффициенты которых органичены многочленом от суммы размеров двоичных записей коэффициентов исходного уравнения.

Ключевые слова: линейное уравнение, двоичное решение, вычислительная сложность.

Для многих задач, хотя известные алгоритмы имеют высокую вычислительную сложность в худшем случае, существуют так называемые генерические алгоритмы, работающие без ошибок и быстро принимающие или отвергающие почти любой вход, но уведомляющие об отказе от решения на малой доле входов [2, 3].

Рассмотрим задачу распознавания: даны $m \times n$ матрица A и вектор $\mathbf{b}$ с целыми коэффициентами, узнать, существует ли $(0,1)$-решение у системы линейных уравнений $A\mathbf{x} = \mathbf{b}$.

В случае, когда все элементы $m \times n$ матрицы A и вектора $\mathbf{b}$ неотрицательные, метод динамического программирования позволяет перечислить все $(0,1)$-решения системы неравенств $A\mathbf{x} \leqslant \mathbf{b}$. Вычислительная сложность линейно зависит от общего числа таких решений. При $m > c\log_2 n$ для некоторой константы c и некоторых предположениях о распределении коэффициентов, среднее число решений полиномиально ограничено, следовательно, все решения легко найти. Доказательство, которое предложил Н. Н. Кузюрин [1], основано на оценке хвостов биномиального распределения. В этом частном случае легко выбрать те $(0,1)$-решения, на которых неравенства обращаются в равенства.

С другой стороны, задача распознавания $(0, 1)$-решения у системы $A\mathbf{x} = \mathbf{b}$ для любых A и $\mathbf{b}$ может быть сведена к ее частному случаю, когда система состоит всего из одного линейного уравнения [4]. Он известен как задача о разбиении множества. Тогда $(0, 1)$-решение одного линейного уравнения может быть найдено за псевдополиномиальное время. Однако в общем случае уравнение имеет большие коэффициенты, следовательно, этот подход не дает эффективного генерического алгоритма.

Случай, когда $2m \leqslant n \leqslant m \log_2 n$ и уравнения линейно независимые, остается вычислительно трудным в худшем случае даже при малых абсолютных величинах коэффициентов всех уравнений системы. Алгебраический подход позволяет уточнить структуру множества трудных входов. Согласно [3], когда число переменных n и число уравнений m удовлетворяют неравенству вида $m > n - \sqrt{2n - o(n)}$, набор трудных входов включается в множество нулей многочлена от коэффициентов уравнений. Этот многочлен отличен от константы и определяется числами n и m. Новый результат уточняет оценку.

Теорема 1. *Существуют сублинейная функция $s = o(n)$ и генерический алгоритм полиномиального времени, который для всех положительных целых чисел n и m, удовлетворяющих неравенству $m > n - \sqrt{6n - s(n)}$, и для почти каждого набора m линейных форм $\ell_j(x_0, \cdots, x_{n-m})$, где $j > n - m$, допускает лишь такой вход, для которого не существует $(0, 1)$-решения системы уравнений $x_j = \ell_j(1, x_1, \cdots, x_{n-m})$. Более того, для указанных n и m этот алгоритм не отвергает вход и существует такой отличный от константы многочлен степени $O(\sqrt{n^3})$ от коэффициентов линейных форм ℓ_j, что, если алгоритм дает уведомление об отказе, то этот многочлен обращается в нуль.*

Хотя все NP-полные задачи сводимы по Карпу друг к другу, образ такой сводимости может составлять малую долю всех случаев. Поэтому полиномиальная в среднем разрешимость некоторой NP-полной задачи не влечет существование такого алгоритма для других задач из класса NP. Рассмотрим пример такой сводимости.

Лемма 2. *Существует такая константа $c > 0$, что за полиномиальное время для данного числа $s \geqslant 2$ можно найти список различных простых чисел p_k, произведение которых превосходит число s, где каждое число удовлетворяет неравенству $p_k < c \log_2 s$.*

Доказательство. Алгоритм реализует решето Эратосфена. Обозначим через $\vartheta(x)$ функцию Чебышева, равную натуральному логарифму произведения простых чисел, которые не превосходят x. Согласно [5], для $x \geqslant 2$ выполнено неравенство

$$|\vartheta(x) - x| \leqslant \frac{151.3x}{\ln^4 x}.$$

Так получается верхняя оценка для простых чисел p_k. □

Теорема 3. *Дано линейное уравнение от n переменных над $\mathbb{Z}$. За полиномиальное время вычислимы матрица A и вектор $\mathbf{b}$ над $\mathbb{Z}$, для которых исходное уравнение и система уравнений $A\mathbf{x} = \mathbf{b}$ имеют одинаковое количество $(0,1)$-решений. Более того, все коэффициенты новой системы неотрицательные и ограничены сверху многочленом от n и общего размера двоичных записей коэффициентов.*

Доказательство. Обозначим через $a_1x_1 + \cdots + a_nx_n = a_0$ исходное уравнение, где все коэффициенты $a_0, \ldots, a_n$ — ненулевые целые числа. Обозначим через s сумму абсолютных величин коэффициентов $s = |a_0| + |a_1| + \cdots |a_n|$. По лемме 2 за полиномиальное время вычисляется список различных простых чисел $p_1 < \cdots < p_r$, удовлетворяющий неравенству $s < p_1 \cdot p_2 \cdots p_{r-1} \cdot p_r$.

По китайской теореме об остатках, исходное уравнение имеет те же $(0,1)$-решения, что и система сравнений от n переменных

$$\begin{cases} a_1x_1 + \cdots a_nx_n & \equiv & a_0 & \pmod{p_1} \\ \cdots & \cdots & \cdots & \cdots \\ a_1x_1 + \cdots a_nx_n & \equiv & a_0 & \pmod{p_r} \end{cases}$$

Обозначим через $a_j \bmod p_k$ остаток от деления числа a_j на p_k, принимающий значения от нуля до $p_k - 1$. В свою очередь, каждое из сравнений $a_1x_1 + \cdots a_nx_n \equiv a_0 \pmod{p_k}$ имеет столько же $(0,1)$-решений, что и следующее уравнение над $\mathbb{Z}$, зависящее от новых переменных $y_{k0}, \ldots, y_{ku}$, где $u = \lfloor \log_2 n \rfloor - 1$,

$$\sum_{j=1}^{n} (a_j \bmod p_k) x_j - p_k \sum_{\ell=0}^{u} 2^\ell y_{k\ell} = a_0 \bmod p_k$$

Так получается система из r уравнений над $\mathbb{Z}$, но к прежним n переменным добавилось еще $r\lfloor \log_2 n \rfloor$ новых переменных. Замена переменных $y_{k\ell} = 1 - x_{k\ell}$, меняет знаки у коэффициентов. □

Пример 1. *Рассмотрим уравнение* $x_1 + x_2 - x_3 = 2$. *Сумма абсолютных величин коэффициентов равна* $s = 5$. *Поэтому достаточно взять два простых числа* $p_1 = 2$ *и* $p_2 = 3$. *Система сравнений*

$$\begin{cases} x_1 + x_2 + x_3 & \equiv & 0 & \pmod 2 \\ x_1 + x_2 + 2x_3 & \equiv & 2 & \pmod 3 \end{cases}$$

сводится к системе уравнений над $\mathbb{Z}$ *с двумя новыми переменными* y_1 *и* y_2, *где каждое уравнение имеет тот же набор* $(0,1)$-*решений, что и соответствующее сравнение*

$$\begin{cases} x_1 + x_2 + x_3 - 2y_1 & = & 0 \\ x_1 + x_2 + 2x_3 - 3y_2 & = & 2 \end{cases}$$

Замена $y_1 = 1 - x_4$ *и* $y_2 = 1 - x_5$ *даст систему с неотрицательными коэффициентами при линейных членах*

$$\begin{cases} x_1 + x_2 + x_3 + 2x_4 & = & 2 \\ x_1 + x_2 + 2x_3 + 3x_5 & = & 5 \end{cases}$$

Исходное уравнение имеет лишь одно $(0,1)$-*решение* $(1,1,0)^T$. *Новая система также имеет одно* $(0,1)$-*решение* $(1,1,0,0,1)^T$.

Если в исходном уравнении из условия теоремы 3 коэффициентами служат случайные целые числа независимо и равномерно распределенные на достаточно большом отрезке, то в новой системе некоторые коэффициенты детерминированы числом переменных и размером записи исходного уравнения, а другие коэффициенты почти равномерно распределены, каждый на своем отрезке от нуля до некоторого числа $p_k - 1$.

Наличие детерминированных коэффициентов приводит к тому, что мало эффективен алгоритм, предложенный Н.Н. Кузюриным [1]. В системе неравенств $A\mathbf{x} \leqslant \mathbf{b}$, соответствующей системе уравнений из теоремы 3, много допустимых $(0,1)$-решений.

Полученные результаты могут быть использованы для тестирования эвристических методов поиска $(0,1)$-решений систем уравнений.

Список литературы

[1] *Кузюрин, Н. Н.* Полиномиальный в среднем алгоритм в целочисленном линейном программировании // Сибирский Журнал Исследования Операций. — 1994. — Т. 1, № 3. — С. 38–48.

[2] *Рыбалов, А. Н.* О генерической сложности проблемы о сумме подмножеств для полугрупп целочисленных матриц // Прикладная Дискретная Математика. — 2020. — № 50. — С. 118–126.

[3] *Селиверстов, А. В.* Двоичные решения для больших систем линейных уравнений // Прикладная Дискретная Математика. — 2021. — № 52. — С. 5–15.

[4] *Селиверстов, А. В.* О двоичных решениях систем уравнений // Прикладная Дискретная Математика. — 2019. — № 45. — С. 26–32.

[5] *Dusart, P.* Explicit estimates of some functions over primes // The Ramanujan Journal. — 2018. — V. 45. — P. 227–251.

Библиографическая ссылка

Селиверстов, А. В. О сводимости систем линейных уравнений // Всероссийская научная конференция «Математические основы информатики и информационно-коммуникационных систем». Сборник трудов. — Тверь : ТвГУ, 2021. — С. 262–266.
https://doi.org/10.26456/mfcsics-21-36

Сведения об авторах

Селиверстов Александр Владиславович
Институт проблем передачи информации им. А. А. Харкевича РАН.
Ведущий научный сотрудник

Россия, 127051, Москва, Большой Каретный пер. 19, стр. 1
E-mail: slvstv@iitp.ru