2. Абросимова А.А., Журавлев В.Г. Двумерное обобщение теоремы Гекке и сбалансированные слова // Алгебра и теория чисел: современные проблемы и приложения: тез. докл. VIII Международной конференции, посвященной 190-летию П.Л. Чебышева и 120-летию И.М. Виноградова — Саратов, 2011. С. 3-4.

3. Мокрова А.А., Журавлев В.Г. Перекладывающиеся полимино с симметриями // Математическая кристаллография и родственные задачи: материалы всерос. конф. с междунар. участием — Владимир, 2023. С. 17-21.

4. Журавлев В.Г., Осипова А.А. Полимино с симметриями: учебное пособие для самостоятельной работы по математике // Автоном. некоммерч. образоват. орг. высш. образования Центросоюза Рос. Федерации «Рос. ун-т кооперации», Владим. фил. – Владимир: ООО «Аркаим», 2016. – 48 с.

5. Осипова А.А., Монатова А.А. Построение перекладывающихся полимино // Актуальные проблемы развития науки и современного образования: сборник материалов Международной научно-практической конференции (Белгород, 10 апреля 2017 г). — Белгород, 2017. С. 57-59.

УДК 512.644

О двоичных решениях у системы нескольких линейных уравнений по модулю три

А. В. Селиверстов (Россия, г. Москва)
Институт проблем передачи информации им. А. А. Харкевича РАН
e-mail: slvstv@iitp.ru

On binary solutions to a system of several linear equations modulo three

A. V. Seliverstov (Russia, Moscow)
Institute for Information Transmission Problems of the RAS (Kharkevich Institute)
e-mail: slvstv@itp.ru

Обозначим через $GF(3)$ поле вычетов по модулю три. Элементы поля $GF(3)$ будем обозначать числами из множества $\{0, 1, 2\}$.

Решение системы уравнений, в котором значение каждой переменной принадлежит множеству $\{0, 1\}$, называется $(0, 1)$-решением или двоичным решением. Распознавание существования $(0, 1)$-решения у системы линейных уравнений над полем $GF(3)$ служит примером NP-полной задачи. Однако для одного уравнения эта задача решается легко: только линейное уравнение вида $x_k = 2$ не имеет $(0, 1)$-решения, поскольку каждое линейное уравнение, нетривиально зависящее от двух или более переменных, имеет $(0, 1)$-решение. Более того, задача поиска $(0, 1)$-решения также разрешима за полиномиальное время для систем из фиксированного числа линейных уравнений. Например, можно использовать сводимость задачи над $GF(3)$ к аналогичной задаче над полем рациональных чисел, для решения которой известно много алгоритмов, см. [1, 2]. Мы же рассмотрим системы, в которых число уравнений ограничено не константой, а монотонно возрастающей функцией от числа переменных. Также обсуждаются вероятностные алгоритмы. Распределение значений сумм случайных $(0, 1)$-величин рассмотрено Яшунским [3].

Пусть система линейных уравнений от переменных $x_1, \ldots, x_n$ содержит больше одного уравнения и некоторое уравнение нетривиально зависит от переменной x_k. Будем говорить, что новая система линейных уравнений получена из исходной системы исключением переменной x_k, если новая система не зависит от переменной x_k, а исходная система эквивалентна объединению новой системы и ровно одного уравнения (зависящего от x_k), равного линейной комбинации уравнений исходной системы.

Исключение переменной может приводить к системе, имеющей большее число $(0,1)$-решений, чем было у исходной системы. Следующий результат справедлив лишь над полем $GF(3)$, но не над полями с большим числом элементов.

Предложение 1. *Даны натуральные числа n и m, удовлетворяющие неравенствам $n \geqslant 5$ и $2 \leqslant m \leqslant \log_3(2n-1)$, и система из m линейных уравнений от n переменных над полем $GF(3)$. Пусть для каждого индекса $1 \leqslant k \leqslant n$ существует уравнение, нетривиально зависящее от x_k. Если у этой системы нет $(0,1)$-решения, то существует такой индекс $1 \leqslant k \leqslant n$, что исключие переменной x_k вновь приводит к системе, у которой нет $(0,1)$-решения. Более того, эта подсистема может быть найдена за полиномиальное время.*

Доказательство.Систему уравнений можно записать в матричном виде $A\mathbf{x} = \mathbf{b}$, где через A обозначена $m \times n$ матрица коэффициентов линейных членов уравнений, а через $\mathbf{x}$ и $\mathbf{b}$ — столбцы из n переменных и m чисел, соответственно. По условию теоремы, в матрице A нет нулевых столбцов.

При условии $2 \leqslant m \leqslant \log_3(2n-1)$ в матрице A найдутся два линейно зависимых столбца. Действительно, число возможных различных ненулевых столбцов равно 3^m-1. Это множество разбивается на $(3^m-1)/2$ пар линейно зависимых столбцов. Поэтому выполнение условия $n \geqslant (3^m+1)/2$ обеспечивает, что в матрице A найдутся два линейно зависимых столбца. Обозначим номера этих столбцов через j и k. Найти номера j и k можно перебирая $n(n-1)/2$ вариантов и проверяя линейную зависимость соответствующих столбцов.

Исходная система $A\mathbf{x} = \mathbf{b}$ эквивалентна системе $B\mathbf{x} = \mathbf{c}$, где в $m \times n$ матрице B в столбцах с номерами j и k ненулевые элементы расположены лишь в одной строке, номер которой обозначим через ℓ. Здесь матрица B получается из матрицы A элементарными операциями над строками, а элемент столбца $\mathbf{c}$ равен соответствующей линейной комбинации элементов столбца $\mathbf{b}$. Если система уравнений, полученная удалением ℓ-го уравнения из этой системы уравнений, имеет $(0,1)$-решение, то она имеет $(0,1)$-решение при любых значениях переменных x_j и x_k. Следовательно, вся система тоже имеет $(0,1)$-решение, поскольку выбор значений переменных x_j и x_k позволяет выполнить ℓ-ое уравнение при любой оценке остальных переменных. Удаление ℓ-го уравнения соответствует исключению каждой из переменных x_j и x_k.

□

Предложение 2. *Существует алгоритм полиномиального времени, который получает на вход систему из m линейных уравнений от n переменных над полем $GF(3)$ и при условии $m \leqslant \log_3 \log_3(2n-1)$ примимает вход тогда и только тогда, когда система имеет $(0,1)$-решение.*

Доказательство.Алгоритм в цикле делает попытки либо удалить уравнение, которое линейно зависит от остальных уравнений, либо исключить переменную в соответствии с предложением 1. Также удаляются из рассмотрения все переменные, которые не входят в новую систему. В случае успеха на очередном шаге будет получена система уравнений, состоящая из меньшего числа уравнений. При этом новая система имеет $(0,1)$-решение тогда и только тогда, когда исходная система имеет $(0,1)$-решение. После выполнения менее m шагов этот процесс останавливается в одном из двух возможных случаев: либо осталось одно уравнение, либо полученная система зависит от малого числа переменных.

Если осталось одно уравнение, то для уравнения вида $x_k = 2$ вход отвергается, а для уравнения другого вида вход принимается.

Если осталось k переменных, а система содержит несколько уравнений и не может быть уменьшена, то происходит разбор 2^k случаев. Оценим сверху число k. Поскольку оставшееся число уравнений не превышает числа m, выполнено неравенство $\log_3(2k-1) < m$. Но по условию применимости алгоритма выполнено $m \leqslant \log_3 \log_3(2n-1)$. Следовательно, выполнены неравенства $(2k-1) < \log_3(2n-1)$ и $k \leqslant 0.5 \log_3(2n-1) < 0.3155 \log_2(2n-1)$. Поэтому число различных $(0,1)$-оценок оставшихся k переменных меньше числа $(2n-1)^{0.3155}$.

□

Если условие $m \leqslant \log_3 \log_3(2n-1)$ из предложения 2 нарушено, то алгоритм всегда даст правильный ответ, но время работы может быть большим. Однако для большой доли случаев среди входов с данными значениями m и n время работы алгоритма будет маленьким даже при более слабом ограничении $m \leqslant \log_3(2n-1)$.

При данных значениях m и n, удовлетворяющих неравенству $m \leqslant \log_3(2n-1)$, почти любая система из m уравнений от n переменных над полем $GF(3)$ будет иметь много $(0,1)$-решений. С другой стороны, при этом условии существование $(0,1)$-решения всегда может быть проверено некоторым алгоритмом за квазиполиномиальное время $n^{O(\log n)}$.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. 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

2. Селиверстов А. В. Обобщение задачи о сумме подмножеств и кубические формы // Журнал вычислительной математики и математической физики. 2023. Том 63, № 1. С. 51–60.

3. Яшунский А. Д. О суммах бернуллиевских случайных величин по модулю 3 // Математические заметки. 2022. Том 111, № 1. С. 154–157. https://doi.org/10.4213/mzm13214

УДК 519.147

Разбиение пространства на поликубы и плотнейшая упаковка пространства поликубами: способ верификации прямой и обратной задачи

К. Г. Серавкин (Россия, г. Владимир)
Владимирский государственный университет
e-mail: seravkin@rambler.ru

Tilings of space with polycubes and the densest polycube packings of space: way to verify direct and inverse problem

K. G. Seravkin (Russia, Vladimir)
Vladimir State University
e-mail: seravkin@rambler.ru

Предложен вариант подтверждения корректности алгоритма перебора трансляционных кубических разбиений пространства на поликубы и алгоритма поиска плотнейших (без пустот) трансляционных кубических упаковок пространства поликубами.