О СИСТЕМАХ НЕСКОЛЬКИХ УРАВНЕНИЙ ПО МОДУЛЮ ТРИ

А.В. Селиверстов, О.А. Зверков

Институт проблем передачи информации им. А.А. Харкевича Российской академии наук,
Большой Каретный переулок 19, с. 1, 127051 Москва, Россия, {slvstv,zverkov}@iitp.ru

Обозначим через $GF(3)$ поле вычетов по модулю три. Мы называем $(0,1)$-решением такое решение системы уравнений, в котором каждая переменная принимает значения из множества $\{0,1\}$. Получены достаточные условия существования $(0,1)$-решения у системы линейных уравнений над полем $GF(3)$, в которой число уравнений мало по сравнению с числом переменных. Новые результаты дополняют ранее полученные [1, 2].

Рассмотрим систему линейных уравнений, нетривиально зависящую от переменной x_k. 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, равного линейной комбинации уравнений исходной системы. В геометрии исключение переменной соответствует проекции на координатное подпространство.

Лемма 1. *Даны натуральные числа n и m, удовлетворяющие неравенствам $n \geqslant 5$, $m \geqslant 2$ и $m \leqslant \log_3(2n-1)$, 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 переменной x_k. Если у этой системы нет $(0,1)$-решения, то существует такой индекс $k \leqslant n$, что исключение переменной x_k приводит к новой системе, у которой нет $(0,1)$-решения. Более того, эта новая система может быть найдена за полиномиальное время $O(mn\log_2(n+1))$.*

Набросок доказательства. Для системы $A\mathbf{x} = \mathbf{b}$ исключаются переменные, соответствующие пропорциональным друг другу столбцам в матрице A. Это возможно над полем $GF(3)$.

Замечание. Лемма 1 позволяет перейти от исходной системы, содержащей достаточно мало уравнений, к новой системе от меньшего числа переменных и с меньшим числом уравнений. Далее неравенство из условия леммы 1 может быть нарушено, что помешает сделать следующий шаг. Поэтому в условии указанной ниже теоремы предполагается выполнение более сильного ограничения. С другой стороны, вычислительные эксперименты со случайными матрицами позволяют надеяться, что такой рекурсивный спуск возможен для почти всех исходных систем при условии типа $m = O(\log_3 n)$, близком к неравенству из леммы 1.

Лемма 2. *Дана система линейных уравнений от n переменных над полем $GF(3)$*

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n &= b_1 \\ \cdots & \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= b_m \end{cases}$$

и целое число $1 \leqslant s \leqslant n$. Эта система имеет $(0,1)$-решение тогда и только тогда, когда $(0,1)$-решение имеет новая система, в которой для каждого $1 \leqslant j \leqslant m$ в j-ом уравнении коэффициент a_{js} при переменной x_s заменяется линейной комбинацией коэффициентов

$$c_j = 2b_j - \sum_{k=1}^{n} a_{jk}.$$

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

Обсуждаемый алгоритм реализован на языке Python. Листинг программы и примеры доступны по адресу http://lab6.iitp.ru/-/havoc. Входом служит $m \times (n+1)$ матрица M. Обозначим через $\mathbf{b}$ последний столбец этой матрицы, а через A подматрицу, расположенную в первых n столбцах, кроме последнего. Столбец $\mathbf{b}$ содержит свободные члены уравнений, а матрица A состоит из коэффициентов линейных членов. Соответствующая система уравнений имеет вид $A\mathbf{x} = \mathbf{b}$.

Если матрица A пустая, то линейные части всех уравнений равны нулю, а сами уравнения превращаются в тождества $0=0$ или ложные равенства $0=1$ или $0=2$. Матрица M изменяется так, что новая система линейных уравнений имеет $(0,1)$-решение тогда и только тогда, когда исходная система уравнений имеет $(0,1)$-решение. При этом числа строк и столбцов никогда не возрастают. В цикле выполняются шаги, соответствующие леммам 1 и 2, пока матрица M не стабилизируется или не будет выполнено дополнительное условие остановки. При этом для полученной системы уравнений существование или отсутствие $(0,1)$-решения легко проверяется при выполнении условий теоремы.

Пример. Системе уравнений от двух переменных x_1 и x_2 над полем $GF(3)$

$$\begin{cases} 2x_1+2x_2 &= 1 \\ x_1+2x_2 &= 1 \end{cases}$$

соответствует расширенная матрица

$$M = \begin{pmatrix} 2 & 2 & 1 \\ 1 & 2 & 1 \end{pmatrix}.$$

Среди первых двух столбцов нет линейно зависимых, но можно применить лемму 2. Столбец

$$\mathbf{c} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

пропорционален первому столбцу в матрице M. Заменяя второй столбец, получаем матрицу

$$\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \end{pmatrix}.$$

Поскольку первые два столбца пропорциональны друг другу, возможно исключение переменных, которое приводит к ложному равенству $0=2$. Следовательно, $(0,1)$-решений нет.

Экспериментально показано, что алгоритм намного эффективнее для разреженных систем уравнений. Более того, метод двоичного поиска позволяет найти некоторое $(0,1)$-решение системы, когда оно существует, хотя перечисление всех $(0,1)$-решений может быть слишком трудным. Это открывает возможность практического использования для решения тех прикладных задач, которые легко свести к поиску $(0,1)$-решения системы линейных алгебраических уравнений, в частности, для решения задач математической биологии.

Работа выполнена с использованием вычислительных ресурсов Межведомственного суперкомпьютерного центра Российской академии наук (МСЦ РАН).

Исследование выполнено за счет гранта Российского научного фонда № 24-44-00099, https://rscf.ru/project/24-44-00099/.

Литература

1. Бойков А. А., Селиверстов А. В. *О кубе и проекциях подпространства* // Вестник Удмуртского университета. Математика. Механика. Компьютерные науки. 2023. Т. 33, № 3. С. 402–415. DOI: 10.35634/vm230302

2. Zverkov O. A., Seliverstov A. V. *Effective lower bounds on the matrix rank and their applications* // Programming and Computer Software. 2023. V. 49, no. 5. P. 441–447. DOI: 10.1134/S0361768823020160