ПРОГРАММИРОВАНИЕ, 2024, № 2, с. 100–107

КОМПЬЮТЕРНАЯ АЛГЕБРА

УДК 004.421.6+512.644

НИЖНИЕ ГРАНИЦЫ ДЛЯ РАНГА МАТРИЦЫ С НУЛЯМИ И ЕДИНИЦАМИ ВНЕ ГЛАВНОЙ ДИАГОНАЛИ

А. В. Селиверстов[a], * (ORCID: 0000-0003-4746-6396),
О. А. Зверков[a], ** (ORCID: 0000-0002-8546-364X)

[a] *Институт проблем передачи информации им. А.А. Харкевича РАН*
127051 Москва, Большой Каретный пер., д. 19, стр. 1, Россия

**E-mail: slvstv@iitp.ru*
***E-mail: zverkov@iitp.ru*

Поступила в редакцию 12.07.2023
После доработки 10.08.2023
Принята к публикации 01.10.2023

Найдена нижняя граница для ранга квадратной матрицы, у которой каждый элемент на главной диагонали отличен от нуля и от единицы, а вне главной диагонали каждый элемент равен либо нулю, либо единице. Ранг такой матрицы не меньше половины порядка матрицы. При дополнительном условии нижняя граница на единицу выше. Это условие означает отсутствие двоичного решения у некоторой вспомогательной системы линейных уравнений. Даны примеры, показывающие достижимость указанной нижней границы. Полученная нижняя граница для ранга позволяет свести задачу о поиске двоичного решения для системы линейных уравнений, в которой число линейно независимых уравнений достаточно велико, к аналогичной задаче от меньшего числа переменных. Найдены ограничения на существование большого множества решений, каждое из которых отличается от двоичного решения значением одной переменной. Отдельно обсуждается возможность для сертификации отсутствия двоичного решения у системы из большого числа линейных алгебраических уравнений. Также даны оценки времени работы для вычисления ранга матрицы в системе компьютерной алгебры SymPy. Показано, что ранг матрицы над полем вычетов по модулю простого числа вычисляется за меньшее время, чем обычно требуется для вычисления ранга матрицы того же порядка над полем рациональных чисел.

Ключевые слова: ранг матрицы, система линейных уравнений, система компьютерной алгебры, SymPy

DOI: 10.31857/S0132347424020133 **EDN:** RNNVQZ

1. ВВЕДЕНИЕ

Обозначим через K поле, вычислимое за полиномиальное время [1], характеристика которого равна либо нулю, либо нечётному простому числу. Решение системы из m уравнений от n переменных называется (0,1)-решением, если каждая переменная принимает одно из двух значений 0 или 1. Решение называется почти-(0,1)-решением, если одна переменная не равна ни 0, ни 1, а каждая из остальных равна 0 или 1.

Система линейных уравнений определяет подпространство в объемлющем аффинном пространстве с фиксированной системой декартовых координат. Мы отождествляем точки со списками элементов поля или со столбцами матрицы. Над неупорядоченным полем понятие многогранника не определено, но мы отождествляем множество вершин единичного куба в n-мерном пространстве с множеством из 2^n точек, координаты которых принадлежат множеству {0,1}. Две вершины этого куба, т.е. две (0,1)-точки, называются смежными, если они различаются по одной координате. Так, (0,1)-решение системы уравнений — вершина этого куба, принадлежащая данному подпространству; почти-(0,1)-решение — точка, лежащая на прямой, проходящей через две смежные вершины единичного куба, но не совпадающая с вершиной. Точка, все координаты которой равны 1/2, служит центром симметрии единичного куба.

Задача распознавания (0,1)-решения эквивалентна задаче о взаимном расположении подпространства и вершин единичного куба. Эта задача NP-полная. Используя оценки ранга матрицы специального вида, мы предлагаем необходимое условие существования достаточно большого набора почти-(0,1)-решений при отсутствии (0,1)-решений у системы уравнений. Существование почти-(0,1)-решений служит препятствием к снижению размерности задачи распознавания (0,1)-решений посредством исключения переменных, т.е. проектирования на координатное подпространство. Поэтому нарушение найденного нами условия означает возможность снижения размерности, следовательно, снижения

вычислительной сложности. Но мы не будем рассматривать задачи перечисления, которые труднее задач распознавания хотя бы одного решения [2, 3].

Недавно были предложены алгоритмы для распознавания (0,1)-решений системы линейных уравнений с целыми коэффициентами: как эвристические при условии малой плотности [4] или для достаточно большого числа уравнений [5, 6], так и недетерминированные с новыми верхними границами вычислительной сложности [7]. Наши новые результаты остаются справедливыми над конечными полями. При этом над конечным полем исключение переменных не сопровождается ростом длины записи коэффициентов уравнений. Поэтому многие вычисления относительно легко выполнить в системах компьютерной алгебры, а их битовая сложность близка к алгебраической сложности. Более того, над конечным полем при фиксированном числе переменных возможен полный перебор [8].

Ранг квадратной матрицы M связан с размерностью аффинной оболочки L точек, соответствующих столбцам матрицы. Если L содержит начало координат, то $\operatorname{rank}(M) = \dim(L)$, иначе $\operatorname{rank}(M) = \dim(L) + 1$.

Ранг $n \times n$ 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 [9, 10]. С другой стороны, сложность вычисления ранга [11] и характеристического многочлена [12, 13] близка к сложности матричного умножения. Также для вычисления нормальной формы Смита целочисленной матрицы известен быстрый вероятностный алгоритм [14]. Вычисление ранга над кольцами без нетривиальных делителей нуля рассмотрено в работе [15]. Для разреженных симметричных матриц удобно использовать необходимое условие невырожденности, использующее многогранник Ньютона для квадратичной формы [16]. Многогранники Ньютона также полезны для решения других задач [17].

Однако на практике вычисление ранга матриц большого порядка требует больших затрат. Поэтому эффективно проверяемые оценки ранга могут быть полезны для различных приложений. Некоторые результаты о ранге матриц были апробированы на конференции по компьютерной алгебре, посвященной памяти Марко Петковшека (Marko Petkovšek) [18].

В разделе 2 представлены новые оценки ранга матрицы и связанные теоретические результаты. В разделе 3 обсуждаются результаты вычислений в системе компьютерной алгебры SymPy. В разделе 4 дано краткое заключение.

2. ТЕОРЕТИЧЕСКИЕ РЕЗУЛЬТАТЫ

Пусть система уравнений от n переменных имеет для каждого индекса $1 \leqslant k \leqslant n$ некоторое почти-(0,1)-решение, у которого значение координаты $x_k \notin \{0,1\}$. Такие решения соответствуют столбцам матрицы, у которой каждый элемент на главной диагонали отличен от нуля и от единицы, а вне главной диагонали равен либо нулю, либо единице. Оценка ранга такой матрицы позволяет оценить размерность аффинного подпространства, заданного исходной системой уравнений.

Теорема 1. *Дана $n \times n$ матрица M над полем K, в которой каждый элемент на главной диагонали отличен от нуля и от единицы, а вне главной диагонали равен либо нулю, либо единице. Ранг матрицы M не меньше числа $n/2$.*

Доказательство. Если $n = 2$, то ранг 2×2 матрицы M не меньше числа $n/2$, поскольку $\operatorname{rank}(M) \geqslant 1$.

Предположим, что для некоторого $n \geqslant 3$ теорема доказана для всех рассматриваемых $m \times m$ матриц порядка $m < n$. Рассмотрим $n \times n$ матрицу M.

Столбец матрицы M соответствует точке на прямой, проходящей через две смежные (0,1)-точки, но не совпадающей с этими (0,1)-точками. Аффинные преобразования вида $x_k \to 1 - x_k$ отображают (0,1)-точки в другие (0,1)-точки, а почти-(0,1)-точки в другие почти-(0,1)-точки. При этих преобразованиях сохраняется размерность подпространства. Преобразование $x_k \to 1 - x_k$ означает замену всех элементов в k-й строке матрицы. Это позволяет перейти от матрицы M к матрице $\widehat{M}$ того же типа, но в последнем столбце матрицы $\widehat{M}$ все элементы, кроме элемента на главной диагонали, равны нулю. Матрица

$$\hat{M} = \left(\begin{array}{ccc|c} & & & 0 \\ & N & & \vdots \\ & & & 0 \\ \hline * & \cdots & * & \alpha \end{array}\right)$$

для некоторого $\alpha \notin \{0,1\}$. Более того, выполнено неравенство $\operatorname{rank}(M) \geqslant \operatorname{rank}(\widehat{M}) - 1$. Но если аффинная оболочка столбцов матрицы M содержит начало координат, то ранг матрицы M может быть меньше ранга матрицы $\widehat{M}$.

Выполняя элементарные преобразования над столбцами матрицы M, получим матрицу

$$\widetilde{M} = \left(\begin{array}{ccc|c} & & & 0 \\ & N & & \vdots \\ & & & 0 \\ \hline 0 & \cdots & 0 & \alpha \end{array}\right)$$

того же ранга. У матриц M и $\widetilde{M}$ могут отличаться лишь нижние строки. В нижней строке матрицы $\widetilde{M}$ за исключением элемента на главной диагонали остальные элементы равны нулю.

Удаляя последний столбец и последнюю строку из матрицы $\widetilde{M}$, мы получим $(n-1)\times(n-1)$ матрицу N меньшего ранга. По предположению индукции, $\operatorname{rank}(N) \geqslant (n-1)/2$. Поэтому выполнено неравенство $\operatorname{rank}(\widetilde{M}) \geqslant n/2$.

Обозначим через L аффинную оболочку столбцов матрицы $\widetilde{M}$. Возможны два случая. Если L проходит через начало координат, то $\operatorname{rank}(\widetilde{M}) = \dim(L)$. В этом случае $\operatorname{rank}(M) \geqslant \dim(L) = \operatorname{rank}(\widetilde{M}) \geqslant n/2$.

Если L не проходит через начало координат, то $\operatorname{rank}(M) \geqslant \operatorname{rank}(\widetilde{M}) - 1 = \operatorname{rank}(N)$. Аффинная оболочка столбцов матрицы N не проходит через начало координат. Вновь применим преобразования вида $x_k \to 1 - x_k$ к матрице N и получим матрицу $\widetilde{N}$ того же типа, но в последнем столбце матрицы $\widetilde{N}$ все элементы, кроме элемента на главной диагонали, равны нулю. Более того, $\operatorname{rank}(N) \geqslant \operatorname{rank}(\widetilde{N})$. Удаляя из матрицы $\widetilde{N}$ последний столбец и последнюю строку, получим $(n-2)\times(n-2)$ матрицу U меньшего ранга. По предположению индукции её ранг ограничен снизу $\operatorname{rank}(U) \geqslant (n-2)/2$. Тогда $\operatorname{rank}(\widetilde{N}) = \operatorname{rank}(U) + 1 \geqslant n/2$. Следовательно, $\operatorname{rank}(M) \geqslant \operatorname{rank}(N) \geqslant \operatorname{rank}(\widetilde{N}) \geqslant n/2$.

Следующий результат показывает, что эта нижняя оценка ранга точная. При этом используется деление на два. Деление на два объясняет предположение, что характеристика поля K не равна двум. Обозначим через $\lceil \cdot \rceil$ результат округления до большего целого.

Теорема 2. *Для любого нечетного n существует такая $n\times n$ матрица M над полем K, что каждый элемент на главной диагонали отличен от нуля и от единицы, вне главной диагонали — равен либо нулю, либо единице, никакая* $(0,1)$*-точка не лежит в аффинной оболочке столбцов матрицы M и выполнено равенство* $\operatorname{rank}(M) = \lceil n/2 \rceil$.

Доказательство. Рассмотрим $n\times n$ матрицу

$$M = \begin{pmatrix} 1/2 & 0 & 1 & 0 & 1 & \cdots & 0 & 1 \\ 0 & -1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 & -1 \end{pmatrix}$$

и через N обозначим $(n-1)\times(n-1)$ подматрицу, получаемую удалением из матрицы M первого столбца и первой строки. Ранги матриц связаны равенством $\operatorname{rank}(M) = \operatorname{rank}(N) + 1$. Матрица N блочно-диагональная с 2×2 блоками, каждый блок вырожденный. Поэтому её ранг равен числу блоков: $\operatorname{rank}(N) = (n-1)/2$. Следовательно, $\operatorname{rank}(M) = \operatorname{rank}(N) + 1 = (n+1)/2 = \lceil n/2 \rceil$.

Каждый столбец матрицы M служит решением для системы из $(n+1)/2$ линейно независимых уравнений

$$\begin{cases} 2x_1 - x_2 - \cdots - x_{2k} - \cdots - x_{n-1} = 1 \\ x_{2k} + x_{2k+1} = 0,\ 1 \leqslant k \leqslant (n-1)/2. \end{cases}$$

Эта система не имеет $(0,1)$-решений. Действительно, из нижних уравнений следует, что $(0,1)$-решение должно бы иметь нулевые координаты, кроме первой. Но это несовместимо с первым уравнением.

Например, для 3×3 матрицы

$$\begin{pmatrix} 1/2 & 0 & 1 \\ 0 & -1 & 1 \\ 0 & 1 & -1 \end{pmatrix}$$

ранг равен двум. Три столбца соответствуют трем точкам на одной прямой L, которая задана системой из двух уравнений

$$\begin{cases} 1 - 2x_1 + x_2 = 0 \\ x_2 + x_3 = 0. \end{cases}$$

Эта система не имеет $(0,1)$-решений.

Для 4×4 матрицы

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 2 & 1 \\ 1 & 0 & 1 & 1/2 \end{pmatrix}$$

ранг равен трём. Четыре столбца соответствуют точкам на плоскости, заданной системой из двух уравнений

$$\begin{cases} x_3 = x_1 + x_2 + 1 \\ x_4 = (-x_1 + x_2 + 1)/2. \end{cases}$$

Эта система не имеет $(0,1)$-решений.

Для 2×2 матриц, в которых каждый элемент на главной диагонали отличен от нуля и от единицы, а вне главной диагонали равен либо нулю, либо единице, ранг равен единице лишь для матриц

$$\begin{pmatrix} 1/\alpha & 1 \\ 1 & \alpha \end{pmatrix},$$

где $\alpha \notin \{0,1\}$. Столбцы соответствуют точкам на прямой, проходящей через начало координат и заданной уравнением $x_2 = \alpha x_1$. Следовательно, если никакая (0,1)-точка не принадлежит прямой, проходящей через точки, соответствующие столбцам матрицы M, то $\operatorname{rank}(M) = 2$.

Теорема 3. *Даны четное число n и $n \times n$ матрица M над полем K, в которой каждый элемент на главной диагонали отличен от нуля и от единицы, а вне главной диагонали равен либо нулю, либо единице. Если никакая* (0,1)*-точка не лежит в аффинной оболочке столбцов матрицы M, то ранг матрицы M не меньше числа* $(n/2) + 1$.

Доказательство. Применение к строкам матрицы преобразований типа $x_k \to 1 - x_k$, как при доказательстве теоремы 1, позволяет перейти от матрицы M к матрице $\widehat{M}$ того же типа, но в последнем столбце матрицы $\widehat{M}$ все элементы, кроме элемента на главной диагонали, равны нулю. Матрица

$$\hat{M} = \left(\begin{array}{ccc|c} & & & 0 \\ & N & & \vdots \\ & & & 0 \\ \hline * & \cdots & * & \alpha \end{array}\right)$$

для некоторого $\alpha \notin \{0,1\}$. Поскольку аффинная оболочка столбцов матрицы M не содержит никакой (0,1)-точки, это верно и для матрицы $\widehat{M}$. При этом ранг не меняется. Поэтому $\operatorname{rank}(M) = \operatorname{rank}(M) = \operatorname{rank}(N) + 1$. По теореме 1, $\operatorname{rank}(N) \geqslant (n-1)/2$. Следовательно, выполнено неравенство $\operatorname{rank}(M) \geqslant (n+1)/2$. Для чётного n это неравенство эквивалентно неравенству $\operatorname{rank}(M) \geqslant (n/2) + 1$.

Теорема 4. *Дана система m линейно независимых линейных уравнений от n переменных, у которой нет* (0,1)*-решений. Если выполнено неравенство $m > (n+1)/2$, то для некоторого индекса $1 \leqslant k \leqslant n$ не существует почти-*(0,1)*-решения, в котором $x_k \notin \{0,1\}$.*

Доказательство. Пусть для каждой переменной существует почти-(0,1)-решение, отличающееся от нуля и от единицы значением этой переменной. Тогда легко составить матрицу M, в которой каждый элемент на главной диагонали отличен от нуля и от единицы, а вне главной диагонали равен либо нулю, либо единице. Поскольку нет (0,1)-решений, $\operatorname{rank}(M) = n - m + 1$. Если число n нечётное, то $n - m + 1 \geqslant n/2$ по теореме 1. Если число n чётное, то $n - m + 1 \geqslant (n/2) + 1$ по теореме 3. В любом случае $m \leqslant (n+1)/2$. Получено противоречие.

Обозначим через $\lfloor n/2 \rfloor$ целую часть числа $n/2$. Геометрическая интерпретация теоремы 4 заключается в следующем. Пусть $s < \lfloor n/2 \rfloor$. В n-мерном аффинном пространстве для каждого s-мерного подпространства L, которое не инцидентно никакой вершине единичного куба, существует забывающая координату проекция на некоторую координатную гиперплоскость, при которой образ подпространства L снова не инцидентен никакой вершине единичного куба. Проекция, забывающая выбранную координату, легко вычисляется. При этом таких проекций, вообще говоря, несколько, но выбор удачной проекции недетерминированный и может иметь высокую вычислительную сложность. В этом смысле обсуждаемый способ понижения размерности задачи напоминает результаты из работы [7]. Однако мы не используем вероятностных методов.

Теорема 5. *Дана система m линейно независимых линейных уравнений от n переменных над полем K. Если выполнены условия: $n = 2m - 1$, у этой системы нет* (0,1)*-решений, но для каждого индекса $1 \leqslant k \leqslant n$ существует почти-*(0,1)*-решение, в котором $x_k \notin \{0,1\}$, то точка* $(1/2, \ldots, 1/2)$*, каждая координата которой равна* $1/2$*, не служит решением системы.*

Доказательство. Предположим, что точка $(1/2, \ldots, 1/2)$ служит решением системы. Тогда множество остальных решений этой системы распадается на пары симметричных решений, переходящих одно в другое при одновременном преобразовании всех координат $x_k \to 1 - x_k$. При этом преобразовании почти-(0,1)-решение переходит в другое почти-(0,1)-решение, у которого та же самая координата отличается от нуля и от единицы. Однако точка $(1/2, \ldots, 1/2)$ остаётся неподвижной.

Подстановкой нулевого значения вместо последней переменной $x_n = 0$ получим новую систему из m уравнений, у которой нет (0,1)-решений, но для каждого индекса $1 \leqslant k \leqslant n-1$ существует почти-(0,1)-решение, в котором значение $x_k \notin \{0,1\}$. В новой системе число линейно независимых уравнений равно m, а число переменных равно $n - 1 = 2m - 2$. Мы получаем противоречие с теоремой 4.

Следующий результат устанавливает взаимную зависимость почти-(0,1)-решений.

Теорема 6. *Если прямая L пересекает три прямые, каждая из которых содержит по две смежных* (0,1)*-точки, но прямая L не инцидентна никакой* (0,1)*-точке, то во всех точках на прямой L координаты, кроме некоторых трех координат, принимают какие-то постоянные значения из множества* $\{0,1\}$.

Доказательство. Без ограничения общности можно считать, что прямая L пересекает первую координатную ось в точке A с координатами $(\alpha, 0, ..., 0)$, у которой все координаты, кроме первой, равны нулю и $\alpha \notin \{0,1\}$. Для некоторого индекса $k \geqslant 2$ прямая L проходит через точку W, у которой все координаты, кроме k-й, принадлежат множеству $\{0,1\}$.

Прямая L состоит из точек $tA + (1-t)W$, где через t обозначен параметр. Если у точки W среди координат, кроме первой, какие-то две координаты равны единице, то эти координаты у любой третьей точки на прямой L тоже отличны и от нуля и от единицы. Однако по условию на прямой L найдётся третья точка, у которой ровно одна координата отлична от нуля и от единицы. Следовательно, у точки W не более трёх координат могут отличаться от нуля, включая первую. Поэтому прямая L лежит в координатном подпространстве размерности не выше трёх.

3. РЕАЛИЗАЦИЯ И ОБСУЖДЕНИЕ

Ранг матрицы быстрее вычисляется над полем $GF(p)$ вычетов по простому модулю p, чем над полем рациональных чисел, ср. [19]. Такие вычисления реализованы во многих системах компьютерной алгебры, например, в SymPy [20].

В системе SymPy 1.12 выполнены вычисления с матрицами, элементы которых независимо и равномерно распределены на конечном наборе значений. Для конечного поля — над множеством всех элементов поля. Матрицы генерировались методом randMatrix. Если время вычисления ранга одной матрицы меньше минуты, то это вычисление повторялось в пяти сериях. Тогда за время вычисления принимался минимум из пяти значений, каждое из которых получено усреднением внутри одной серии вычислений. Длина такой серии зависит от времени вычисления. Если время одного вычисления превышает две секунды, то каждая серия состоит из одного вычисления. Для каждого порядка матрицы вычислялась медиана по вычислениям для 25 матриц.

Вычисление ранга $n \times n$ матрицы над полем $GF(p)$ для $p \leqslant 11$ и $n \leqslant 500$ требует менее двух минут, а для $n \leqslant 1000$ требует менее 15 минут. При этом медиана времени вычисления ранга монотонно возрастает при увеличении порядка матрицы как $c(p)n^{3+\varepsilon}$, где в зависимости от простого числа p добавка в показателе степени меняется в интервале $0.05 < \varepsilon < 0.09$. Эта медиана монотонно возрастает при увеличении модуля p. Результаты вычислений для $p \in \{3,5,7,11\}$ показаны в табл. 1. Для $n = 500$ и при больших значениях $p \in \{31,101,307,1009,3001\}$ время вычисления ранга мало зависит от величины p. В табл. 2 для тех же данных показаны отношения межквартильного размаха $(Q_3 - Q_1)$ к медиане.

Таблица 1. Медиана времени в секундах для вычисления ранга случайной $n \times n$ матрицы над полем $GF(p)$ для $p \in \{3,5,7,11\}$

n	$GF(3)$	$GF(5)$	$GF(7)$	$GF(11)$
100	0.4	0.5	0.6	0.7
200	3.2	4.6	5.1	5.9
300	11	16	18	21
400	27	39	45	51
500	53	78	91	102
600	95	137	158	177
700	151	220	251	280
800	227	327	376	421
900	324	468	538	595
1000	447	644	737	832

Таблица 2. Отношения межквартильного размаха $(Q_3 - Q_1)$ к медиане времени для вычисления ранга случайной $n \times n$ матрицы над полем $GF(p)$ для $p \in \{3,5,7,11\}$

n	$GF(3)$	$GF(5)$	$GF(7)$	$GF(11)$
100	0.06	0.09	0.10	0.06
200	0.03	0.07	0.07	0.07
300	0.05	0.03	0.03	0.03
400	0.04	0.03	0.02	0.02
500	0.02	0.02	0.02	0.03
600	0.03	0.02	0.02	0.02
700	0.01	0.01	0.01	0.01
800	0.02	0.02	0.01	0.02
900	0.01	0.01	0.01	0.02
1000	0.02	0.01	0.01	0.01

Для матриц над полем рациональных чисел (в SymPy это домен QQ) время вычисления ранга быстрее возрастает при увеличении порядка матрицы, а также зависит от длины двоичной записи элементов матрицы. Генерировались матрицы, элементы которых независимо и равномерно распределены на множестве целых чисел от нуля до 10^k для значений показателя $k \in \{1,2,3,4,5\}$. При этом медиана времени вычисления ранга монотонно возрастает при увеличении порядка матрицы как $c(k)n^{4+\varepsilon}$, где в зависимости от k добавка в показателе степени меняется в интервале $0 < \varepsilon < 0.4$. Для $k = 1$ и $n = 1000$ измеренное время вычисления ранга $n \times n$ матрицы не превышает получаса, а для $k = 5$ — около трёх часов. Результаты приведены в табл. 3.

Таблица 3. Медиана времени в секундах для вычисления ранга случайной $n \times n$ матрицы с целочисленными элементами, которые независимо и равномерно распределены на отрезке от нуля до 10^k для $k \in \{1,2,3,4,5\}$

n	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$
100	0.184	0.262	0.345	0.426	0.513
200	2.20	3.64	5.11	6.71	8.48
300	10.5	18.3	27.0	36.5	47.2
400	32.9	60.2	91.2	126	164
500	83.9	155	237	332	439
600	178	340	526	743	990
700	341	662	1040	1480	1980
800	609	1190	1880	2700	3630
900	1010	2000	3190	4600	6220
1000	1610	3200	5140	7440	10100

Вычисления проведены на персональном компьютере на базе процессора Intel® Core i7-5820K @ 3.30GHz и с оперативной памятью 32 гигабайта.

Обсуждаемое уменьшение числа переменных в задаче поиска (0,1)-решения можно пояснить через диалог между пользователем с малыми возможностями и веб-сервисом с большими возможностями для вычислений. Пользователь получает указания в виде сообщений небольшой длины, но хочет проверить наличие или отсутствие (0,1)-решения у системы линейных уравнений, не доверяя этому сервису. Если (0,1)-решение существует, то оно предъявляется и легко проверить, что указанная последовательность нулей и единиц служит решением. Если (0,1)-решения нет, то подсказка состоит в выборе переменных, которые можно исключить, чтобы новая система по-прежнему не имела (0,1)-решения. Исключение указанных переменных легко выполняется. По теореме 4 число переменных можно уменьшать, если исходная система имеет достаточно много линейно независимых уравнений. В результате система иногда сводится к одному уравнению. Если дальнейшее уменьшение числа переменных невозможно, то пользователю сообщают набор почти-(0,1)-решений. Тогда легко проверить, что нельзя дальше упростить систему. Теорема 2 показывает, что препятствия к упрощению существуют. В худшем случае задача остаётся вычислительно трудной.

4. ЗАКЛЮЧЕНИЕ

Изложенные результаты согласуются с общепринятой гипотезой о высокой вычислительной сложности задач распознавания (0,1)-решений для системы линейных уравнений, поскольку изменение задачи посредством исключения переменных встречает препятствие в худшем случае. Но полученные оценки оставляют возможность для некоторого понижения вычислительной сложности над конечными полями. С другой стороны, системы компьютерной алгебры позволяют быстро вычислять ранг матрицы и размерность аффинного подпространства над полем вычетов по простому модулю.

СПИСОК ЛИТЕРАТУРЫ

1. *Алаев П.Е.* Конечно порожденные структуры, вычислимые за полиномиальное время // Сибирский математический журнал. 2022. Т. 63. № 5. С. 953–974.
2. *Леонтьев В.К., Гордеев Э.Н.* О числе решений системы булевых уравнений // Автоматика и телемеханика. 2021. № 9. С. 150–168. DOI:10.31857/S0005231021090063
3. *Гордеев Э.Н., Леонтьев В.К.* О числе решений диофантова уравнения и проблеме Фробениуса // Журнал Вычислительной Математики и Математической физики, 2022. Т. 62. № 9. С. 1447–1457.
4. *Pan Y., Zhang F.* Solving low-density multiple subset sum problems with SVP oracle // Journal of Systems Science and Complexity. 2016. V. 29. P. 228–242. DOI:10.1007/s11424-015-3324-9
5. *Селиверстов А.В.* Двоичные решения для больших систем линейных уравнений // Прикладная Дискретная Математика. 2021. № 52. С. 5–15. DOI:10.17223/20710410/52/1
6. *Селиверстов А.В.* Обобщение задачи о сумме подмножеств и кубические формы // Журнал вычислительной математики и математической физики. 2023. Т. 63. № 1. С. 51–60.
7. *Akmal S., Chen L., Jin C., Raj M., Williams R.* Improved Merlin–Arthur protocols for central problems in fine-grained complexity // Algorithmica. 2023. V. 85. P. 2395–2426. DOI:10.1007/s00453-023-01102-6
8. *Stoichev S.D., Gezek M.* Unitals in projective planes of order 25 // Mathematics in Computer Science. 2023. V. 17. No. 5. P. 1–19. DOI:10.1007/s11786-023-00556-9
9. *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. DOI:10.1007/BFb0028792
10. *Mulmuley K.* A fast parallel algorithm to compute the rank of a matrix over an arbitrary field // Combinatorica. 1987. V. 7. No. 1. P. 101–104. DOI:10.1007/BF02579205
11. *Cheung H.Y., Kwok T.C., Lau L.C.* Fast matrix rank algorithms and applications // Journal of the ACM.

2013. V. 60. No. 5. Article No. 31. P. 1–25. DOI:10.1145/2528404
12. *Переславцева О.Н.* О вычислении характеристического полинома матрицы // Дискретная математика. 2011. Т. 23. № 1. С. 28–45. DOI:10.4213/dm1128
13. *Neiger V., Pernet C.* Deterministic computation of the characteristic polynomial in the time of matrix multiplication // Journal of Complexity. 2021. V. 67. No. 101572. P. 1–35. DOI:10.1016/j.jco.2021.101572
14. *Birmpilis S., Labahn G., Storjohann A.* A fast algorithm for computing the Smith normal form with multipliers for a nonsingular integer matrix // Journal of Symbolic Computation. 2023. V. 116. P. 146–182. DOI:10.1016/j.jsc.2022.09.002
15. *Abramov S.A., Petkovšek M., Ryabenko A.A.* On ranks of matrices over noncommutative domains // Журнал вычислительной математики и математической физики. 2023. Т. 63. № 5. С. 760–762.
16. *Юран А.* Многогранники Ньютона невырожденных квадратичных форм // Функциональный анализ и его приложения. 2022. Т. 56. № 2. С. 92–100. DOI:10.4213/faa3957
17. *Батхин А.Б., Брюно А.Д.* Вещественная нормальная форма бинарного многочлена в критической точке второго порядка // Журнал вычислительной математики и математической физики. 2023. Т. 63. № 1. С. 3–15.
18. *Seliverstov A.V.* On a simple lower bound for the matrix rank // Компьютерная алгебра: материалы 5-й международной конференции. Москва, 26–28 июня 2023 г. / отв. ред. С.А. Абрамов, А.Б. Батхин, Л.А. Севастьянов. М.: ИПМ им. М.В. Келдыша, 2023. С. 126–128.
19. *Байрамов Р.Э., Блинков Ю.А., Левичев И.В., Малых М.Д., Мележик В.С.* Аналитическое исследование кубатурных формул на сфере в системах компьютерной алгебры // Журнал вычислительной математики и математической физики. 2023. Т. 63. № 1. С. 93–101.
20. *Meurer A., Smith C.P., Paprocki M., Čertik O., Kirpichev S.B., Rocklin M., Kumar A., Ivanov S., Moore J.K., Singh S., Rathnayake T., Vig S., Granger B.E., Muller R.P., Bonazzi F., Gupta H., Vats S., Johansson F., Pedregosa F., Curry M.J., Terrel A.R., Roučka Š., Saboo A., Fernando I., Kulal S., Cimrman R., Scopatz A.* SymPy: symbolic computing in Python // PeerJ Computer Science. 2017. V. 3. No. e103. P. 1–27. DOI:10.7717/peerj-cs.103

LOWER BOUNDS FOR THE RANK OF A MATRIX WITH ZEROS AND ONES OUTSIDE THE LEADING DIAGONAL

A. V. Seliverstov[a], O. A. Zverkov[a]

[a] *Institute for Information Transmission Problems of the Russian Academy of Sciences (Kharkevich Institute), Bolshoy Karetny per. 19, build. 1, Moscow 127051 Russia*

We have found a lower bound on the rank of a square matrix, where every entry in the leading diagonal is neither zero nor one, but every entry outside the leading diagonal is either zero or one. The rank of such a matrix is at least half the order of the matrix. Under an additional condition, the lower bound is one higher. This condition means that some auxiliary system of linear equations has no binary solution. Examples are given showing the achievability of the lower bound. This lower bound on the rank allows us to reduce the problem of finding a binary solution to a system of linear equations, where the number of linearly independent equations is sufficiently large, to a similar problem in a smaller number of variables. Restrictions on the existence of a large set of solutions are found, each of which differs from binary one by the value of one variable. In addition, we discuss the possibility of certifying the absence of a binary solution to a system of a large set of linear algebraic equations. Estimates of the running time for calculating the rank of a matrix with the SymPy computer algebra system are also given. It is shown that the matrix rank over the field of residues modulo a prime number is calculated in less time than is usually required to calculate the rank of a matrix of the same order over the field of rational numbers.

Keywords: matrix rank, system of linear equations, computer algebra system, SymPy

REFERENCES

1. *Alaev P.E.* Finitely generated structures computable in polynomial time // Siberian Mathematical Journal. 2022. V. 63. № 5. P. 801–818. DOI:10.1134/S0037446622050019
2. *Leontiev V.K., Gordeev E.N.* On the number of solutions to a system of Boolean equations // Automation and Remote Control. 2021. V. 82. no. 9. P. 1581–1596. DOI:10.1134/S000511792109006X
3. *Gordeev E.N., Leont'ev V.K.* On the number of solutions to linear Diophantine equation and Frobenius problem. Computational Mathematics and Mathematical Physics. 2022. V. 62. № 9. P. 1413–1423. DOI:10.1134/S0965542522090044
4. *Pan Y., Zhang F.* Solving low-density multiple subset sum problems with SVP oracle // Journal of Systems Science and Complexity. 2016. V. 29. P. 228–242. DOI:10.1007/s11424-015-3324-9

5. *Seliverstov A.V.* Binary solutions to large systems of linear equations // Prikladnaya Diskretnaya Matematika. 2021. № 52. P. 5–15 (in Russian). DOI:10.17223/20710410/52/1
6. *Seliverstov A.V.* Generalization of the subset sum problem and cubic forms // Computational Mathematics and Mathematical Physics. 2023. V. 63. № 1. P. 48–56. DOI:10.1134/S0965542523010116
7. *Akmal S., Chen L., Jin C., Raj M., Williams R.* Improved Merlin–Arthur protocols for central problems in fine-grained complexity // Algorithmica. 2023. V. 85. P. 2395–2426. DOI:10.1007/s00453-023-01102-6
8. *Stoichev S.D., Gezek M.* Unitals in projective planes of order 25 // Mathematics in Computer Science. 2023. V. 17. № 5. P. 1–19. DOI:10.1007/s11786-023-00556-9
9. *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. DOI:10.1007/BFb0028792
10. *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. DOI:10.1007/BF02579205
11. *Cheung H.Y., Kwok T.C., Lau L.C.* Fast matrix rank algorithms and applications // Journal of the ACM. 2013. V. 60, no. 5. Article no. 31. P. 1–25. DOI:10.1145/2528404
12. *Pereslavtseva O.N.* Calculation of the characteristic polynomial of a matrix // Discrete Mathematics and Applications. 2011. V. 21. № 1. P. 109–128. DOI:10.1515/DMA.2011.008
13. *Neiger V., Pernet C.* Deterministic computation of the characteristic polynomial in the time of matrix multiplication // Journal of Complexity. 2021. V. 67. № 101572. P. 1–35. DOI:10.1016/j.jco.2021.101572
14. *Birmpilis S., Labahn G., Storjohann A.* A fast algorithm for computing the Smith normal form with multipliers for a nonsingular integer matrix // Journal of Symbolic Computation. 2023. V. 116. P. 146–182. DOI:10.1016/j.jsc.2022.09.002
15. *Abramov S.A., Petkovšek M., Ryabenko A.A.* On ranks of matrices over noncommutative domains // Computational Mathematics and Mathematical Physics. 2023. V. 63. № 5. P. 771–778. DOI:10.1134/S0965542523050020
16. *Yuran A.Y.* Newton polytopes of nondegenerate quadratic forms // Functional Analysis and Its Applications. 2022. V. 56. № 2. P. 152–158. DOI:10.1134/S0016266322020095
17. *Batkhin A.B., Bruno A.D.* Real normal form of a binary polynomial at a second-order critical point // Computational Mathematics and Mathematical Physics. 2023. V. 63. № 1. P. 1–13. DOI:10.1134/S0965542523010062
18. *Seliverstov A.V.* On a simple lower bound for the matrix rank. In: S.A. Abramov, A.B. Batkhin, L.A. Sevastyanov (eds.) Computer algebra: 5th International Conference Materials. Moscow, 26–28 June, 2023. Moscow: KIAM, 2023. P. 126–128.
19. *Bairamov R.E., Blinkov Yu.A., Levichev I.V., Malykh M.D., Melezhik V.S.* Analytical study of cubature formulas on a sphere in computer algebra systems // Computational Mathematics and Mathematical Physics. 2023. V. 63. № 1. P. 77–85. DOI:10.1134/S0965542523010050
20. *Meurer A., Smith C.P., Paprocki M., Čertik O., Kirpichev S.B., Rocklin M., Kumar A., Ivanov S., Moore J.K., Singh S., Rathnayake T., Vig S., Granger B.E., Muller R.P., Bonazzi F., Gupta H., Vats S., Johansson F., Pedregosa F., Curry M.J., Terrel A.R., Roučka Š., Saboo A., Fernando I., Kulal S., Cimrman R., Scopatz A.* SymPy: symbolic computing in Python // PeerJ Computer Science. 2017. V. 3. № e103. P. 1–27. DOI:10.7717/peerj-cs.103