ФГБОУ ВПО «Московский государственный
университет имени М.В. Ломоносова»

На правах рукописи

УДК 512.643

Будревич Михаил Вячеславович

О КОНВЕРТАЦИИ ПЕРМАНЕНТА И ОПРЕДЕЛИТЕЛЯ

01.01.06 — математическая логика, алгебра и теория чисел

диссертация на соискание ученой степени
кандидата физико-математических наук

Научный руководитель
доктор физико-математических наук
профессор А.Э. Гутерман

Москва, 2014

Оглавление

Введение

Общая характеристика работы

Актуальность темы исследования

Перманент квадратной матрицы $A = (a_{ij})$ порядка n определяется следующим образом:

$$\mathrm{per}\,(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i\sigma(i)},$$

где S_n это группа перестановок порядка n.

Формула перманента матрицы отличается от определителя матрицы отсутствием умножения на знак перестановки, поэтому его иногда называют “определителем без знака”.

Впервые перманент, как класс симметрических функций, был независимо введен Коши [16] и Бине [10]. Термин “перманент” для квадратных матриц был введен Мюиром [34]. Кроме того, Мюир доказал базовые свойства перманента по аналогии с определителем, впервые исследуя эти понятия как родственные. В работах Литлвуда и Ричардсона [27, 28] понятия перманента и определителя были обобщены до иммананта, в котором слагаемые берутся с коэффициентом, равным значению фиксированного характера на соответствующей перестановке.

Полиа предложил другой подход, связывающий вычисление перманента и определителя матрицы [36]. Например, для матриц порядка $n = 2$ имеет место равенство:

$$\mathrm{per} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \det \begin{pmatrix} a_{11} & -a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

Он также сформулировал следующую задачу, известную как проблема Полиа знаковой конвертации перманента матриц:

Проблема 1. Когда для произвольной матрицы A порядка n выполнено равенство

$$\mathrm{per}\,(A) = \det\,(A'), \tag{1}$$

где матрица A' получена из A путем умножения некоторых элементов матрицы на -1?

Если существует такой способ умножения некоторых элементов на -1, при котором выполнено равенство (1), будем говорить, что матрица A знаково конвертируемая, в противном случае матрица называется знаково неконвертируемой. Далее в тексте под конвертацией матриц мы будем подразумевать знаковую конвертацию, если не оговорено противное. Известно, что существуют, как конвертируемые, так и неконвертируемые матрицы (см., например, [39]).

Следующим важным результатом является необходимое условие конвертации в терминах числа ненулевых элементов для (0,1)-матриц, доказанное Гибсоном:

Теорема 2 (Гибсон, [22])**.** Пусть $A \in M_n(0,1)$ — конвертируемая матрица и $\mathrm{per}\,(A) > 0$. Тогда в матрице A не более, чем $\Omega_n = \frac{n^2+3n-2}{2}$ единичных элементов. Более того, если число единичных элементов в точности равно

Ω_n, то существуют матрицы перестановок P и Q такие, что

$$PAQ = G_n = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ 1 & 1 & 1 & 0 & \dots & 0 & 0 \\ 1 & 1 & 1 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & 1 & \dots & 1 & 0 \\ 1 & 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & 1 & 1 & 1 & \dots & 1 & 1 \end{pmatrix}$$

Знаковой схемой матрицы A называется матрица $\mathrm{sign}(A)$, в которой все элементы заменены на их знак. Матрица A называется знаково невырожденной, если любая матрица с аналогичной знаковой схемой обратима. Бруалди и Шейдер [14] доказали, что вопрос о конвертации (0,1)-матрицы A эквивалентен вопросу о существовании знаково невырожденной матрицы с тем же расположением ненулевых элементов. В частности, из этого следует, что неотрицательная матрица A конвертируема тогда и только тогда, когда конвертируема матрица A', полученная из A заменой всех ненулевых элементов на единичные. Знаковая невырожденность связана с понятием знаковой разрешимости систем линейных уравнений, применяемым в задачах статистики и прогнозирования [15].

По (0,1)-матрице A построим двудольный граф $G = (U, V)$ такой, что ребро (u_i, v_j) принадлежит G тогда и только тогда, когда $a_{ij} = 1$. Литтл в [26] установил, что проблема Полиа о конвертации (0,1)-матрицы A алгоритмически эквивалента задаче о существовании пфаффиановой ориентации двудольного графа G.

Вазирани и Янакакис [44] доказали, что проблема Полиа для (0,1)-матриц эквивалентна задаче поиска цикла четной длины в ориентированном графе и задаче о проверке равенства $\mathrm{per}\,(A) = \det\,(A)$ для неотрицательных матриц. В [33, 37] были независимо предложены полиномиальные алгоритмы для проверки существования пфаффиановой ориентации двудольного графа G.

Можно выделить два направления исследований проблемы Полиа. Первое активно развивающееся направление берет свое начало в теории матриц [4, 5, 6, 9, 30, 20] и связано с построением общей теории конвертации для произвольных иммanантов, обобщающих понятие перманента и определителя. Второе направление исследований отталкивается от задач теории графов и связано с построением теории конвертации перманента для (0,1)-матриц [26, 33, 44].

Важную роль перманент играет и в теории сложности, так как реализует число решений многих комбинаторных задач. Одним из минимальных по сложности (из известных) является алгоритм вычисления перманента, предложенный Райзером (см. [7], глава 7, пункт 2). Алгоритм Райзера имеет экспоненциальную сложность. Более того, классическим является результат Валианта [43], который показал, что вычисление перманента (0,1)-матрицы лежит в классе $\#$-P сложных задач [29].

Таким образом, исследования различных способов вычисления перманента, в том числе с помощью конвертации, мотивированы использованием этой функции в прикладных задачах и активно разрабатываются. Поэтому, исследование конвертируемости перманента матриц для различных подмножеств кольца матриц представляет не только самостоятельный теоретический интерес, но и является эффективным инструментом при работе с различными классами вычислительных задач в прикладной алгебре, теории графов и комбинаторике. Этим объясняется актуальность настоящей работы.

Цель работы

Исследование свойства конвертируемости неотрицательных матриц при выполнении матричных операций. Исследование свойств тензора перманента и доказательство запрета на существование биективных отображений, переводящих перманент в определитель матрицы в случае матриц над конечным полем.

Научная новизна

Полученные в работе результаты являются новыми. Среди них:

- Получено необходимое и достаточное условие конвертируемости суммы матриц и необходимое условие конвертируемости произведения матриц. Полностью охарактеризованы все конвертируемые матрицы, полученные кронекеровым произведением.
- Решен ряд проблем конвертируемости перманента (0,1)-матриц с некоторыми специальными условиями. В том числе:
  - Решена проблема, поставленная в работах [4, 5], о существовании конвертируемых и неконвертируемых (0,1)-матриц с числом единиц между границами конвертации.
  - Найдено минимальное количество единиц во вполне неразложимой неконвертируемой (0,1)-матрице.
- Доказано достаточное условие знаковой конвертируемости матрицы над конечным полем.
- Исследован вопрос о биективной конвертации для матриц над конечным полем, в том числе получены следующие результаты:
  - Введен и исследован тензор перманента и его свойства.

- Доказано, что над конечным полем $\mathbb{F}$ с $\mathrm{char}(\mathbb{F}) > 2$ количество матриц порядка $n \geq 3$ с нулевым определителем больше, чем количество матриц с нулевым перманентом.
- Доказано, что не существует биективного отображения, позволяющего заменить вычисление перманента на вычисление определителя.

Основные методы исследования

Наряду с классическими методами и результатами линейной алгебры, используются также комбинаторные методы, ориентированные на исследование функции перманента. Автором введено понятие тензора перманента, которое является основным инструментом для оценки числа матриц с нулевым перманентом над конечным полем.

Теоретическая и практическая значимость

Работа имеет теоретический характер. Полученные в ней результаты могут быть использованы в различных задачах теории колец, линейной алгебры, вычислительных методов.

Апробация результатов

Результаты диссертации неоднократно докладывались на научно-исследовательских семинарах: научно-исследовательские семинары по алгебре кафедры Высшей алгебры МГУ, “Кольца и модули”, “Теория матриц”, семинары кафедр Математической теории интеллектуальных систем и Дифференциальной геометрии и приложений в 2011-2014 годах.

Также результаты докладывались на следующих конференциях:

- XIX международной конференции студентов, аспирантов и молодых ученых “Ломоносов-2012”, Москва, 2012.

- XXI международной конференции студентов, аспирантов и молодых ученых “Ломоносов-2014”, Москва, 2014.
- $7^{\text{ой}}$ симпозиум по линейной алгебре, Любляна, Словения, 4-12 июня 2014.
- $10^{\text{ая}}$ международная конференция по конечным полям и их приложениям, Гент, Бельгия, 11-15 июля 2011.

Структура диссертации

Диссертация состоит из введения, трех глав, разбитых на параграфы, списка литературы и списка публикаций автора. Общий объем работы составляет 122 страницы. Список литературы включает 44 наименования.

Публикации

Результаты диссертации опубликованы в 7 работах автора.

Краткое содержание работы

Введение. Во введении изложена краткая история вопроса, показана актуальность рассматриваемых задач. Сформулированы цель работы и основные результаты.

Глава 1 посвящена изучению вопроса сохранения свойства конвертируемости матриц при выполнении различных операций над ними. Под конвертируемостью понимается:

Определение. Квадратная матрица $A \in M_n$ порядка n называется конвертируемой, если существует матрица $X \in M_n(\pm 1)$ такая, что выполнено равенство $\text{per}\,(A) = \det\,(A \circ X)$.

Операция “$\circ$” означает поэлементное умножение матриц.

В разделе 1.3 рассматриваются операции сложения и умножения неотрицательных матриц. Для неотрицательной матрицы A через $\phi(A)$ обозначена матрица, полученная из A заменой всех ненулевых элементов на единицы. Доказано необходимое и достаточное условие конвертируемости суммы матриц.

Теорема (1.3.13) Пусть A, B — вещественные неотрицательные квадратные матрицы с положительным перманентом. Тогда матрица $(A + B)$ конвертируема в том и только в том случае, когда существует конвертируемая матрица $C \in M_n(0, 1)$ такая, что $\phi(A) \leq C$ и $\phi(B) \leq C$.

Для произведения матриц доказано, что если одна из матриц неконвертируема, а перманент второй отличен от нуля, то произведение неконвертируемо. Также установлено необходимое условие конвертируемости произведения матриц, когда один из сомножителей является максимальной конвертируемой матрицей. Неотрицательная матрица называется максимальной конвертируемой, если при замене любого нулевого элемента на положительный получится неконвертируемая матрица.

Следствие (1.3.21) Пусть A, B — неотрицательные матрицы, где A — максимальная конвертируемая матрица и существуют, матрицы перестановок P, Q такие, что $\phi(B) \geq P(U_{m,n} + I_n)Q$, $m \geq 3$. Тогда матрицы BA и AB — неконвертируемые.

В последней теореме через $U_{m,n} \in M_n(0, 1)$ обозначена матрица следующего вида:

$$u_{ij} = \begin{cases} 1, \text{ если } 2 \leq j = i + 1 \leq m \\ 1, \text{ если } i = m, j = 1 \\ 0, \text{ иначе.} \end{cases}$$

В разделе 1.4 изучается кронекерово произведение неотрицательных матриц. Кронекеровым произведением матриц $A = (a_{ij})$ и $B = (b_{ij})$ называется блочная матрица

$$A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \dots & \dots & \dots \\ a_{n1}B & \dots & a_{nn}B \end{pmatrix}.$$

Доказано необходимое и достаточное условие конвертируемости кронекерового произведения.

Теорема (1.4.17) Пусть $A \in M_n(0,1)$ и $B \in M_m(0,1)$, и перманент матриц A и B отличен от нуля. Тогда кронекерово произведение $A \otimes B$ конвертируемо в том и только в том случае, когда одна из матриц содержит единственную обобщенную диагональ без нулевых элементов, а вторая матрица конвертируема.

В **главе 2** изучается вопрос построения конвертируемых и неконвертируемых (0,1)-матриц при различных ограничениях.

Через $SM_n \subset M_n$ будем обозначать подмножество симметричных матриц.

Определение (2.1.8) Матрица $A \in SM_n(0,1)$ называется симметрично конвертируемой, если существует матрица $X \in SM_n(\pm 1)$ такая, что $\mathrm{per}\,(A) = \det\,(A \circ X)$. Матрица $A \in SM_n(0,1)$ называется слабо симметрично конвертируемой, если существует симметричная матрица $X \in SM_n(\pm 1)$ такая, что $\mathrm{per}\,(A) = \pm\det\,(A \circ X)$.

Каждой матрице $A \in M_n(0,1)$ сопоставим пару чисел (n,r), где первое число — порядок матриц, а второе — количество единиц в матрице. Число Ω_n, называемое верхней границей конвертации, равно такому максимальному количеству единиц в (0,1)-матрице с положительным перманентом, при котором она может быть конвертируемой. Число ω_n, называемое нижней границей конвертации, равно такому минимальному количеству единиц в (0,1)-матрице, при котором матрице может быть неконвертируемой.

В разделе 2.2 изучался вопрос о существовании слабо симметрично неконвертируемых (0,1)-матриц порядка $n \geq 3$ для различных значений параметра $r \in [\omega_n, \Omega_n]$, равного числу единиц в матрице.

Теорема (2.2.4) Для любого $n \geq 3$ и для любого $r \in [\omega_n, \Omega_n]$ существует слабо симметрично неконвертируемая симметричная (0,1)-матрица типа (n, r).

В разделе 2.3 исследован вопрос о числе ненулевых элементов (0,1)-матрицы, при котором вполне неразложимая матрица всегда конвертируема.

Матрица A называется частично разложимой, если существуют матрицы перестановок P, Q такие, что PAQ — блочная верхнетреугольная матрица. В противном случае будем говорить, что матрица A вполне неразложима. Если существует матрица перестановок P, такая, что $P^t AP$ — блочная верхнетреугольная матрица, то матрица называется разложимой, и неразложимой, если такой P не существует.

Для доказательства основного результата этого раздела введено понятие свертки матрицы, которое в некоторых случаях позволяет перейти к исследованию проблемы Полиа для матриц меньшего порядка:

Определение (2.3.12) Пусть в первой строке неотрицательной матрицы только два ненулевых элемента a_{11}, a_{12}. Сверткой матрицы A по первой строке назовем неотрицательную матрицу $\mathfrak{S}(A)$ следующего вида:

$$\mathfrak{S}(A) = \begin{pmatrix} a_{11}a_{22} + a_{12}a_{21} & a_{23} & \dots & a_{2n} \\ a_{11}a_{32} + a_{12}a_{31} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots \\ a_{11}a_{n2} + a_{12}a_{n1} & a_{n3} & \dots & a_{nn} \end{pmatrix}$$

Определение свертки очевидно обобщается на произвольную строку с двумя ненулевыми элементами. Доказаны следующие свойства операции свертки:

Лемма (2.3.14) Пусть $A \in M_n(\mathbb{R}_+)$ и существует ее свертка по первой строке, равная матрице $\mathfrak{S}(A)$. Если матрица $\mathfrak{S}(A)$ конвертируема, то конвертируема и матрица A.

Лемма (2.3.15) Пусть $A \in M_n(\mathbb{R}_+)$ и существует ее свертка по первой строке, равная матрице $\mathfrak{S}(A)$. Тогда, если матрица A конвертируема, то конвертируема и матрица $\mathfrak{S}(A)$.

Для $A \in M_n(0,1)$ через $\nu(A)$ обозначим число единиц в матрице A. Основным результатом раздела 2.3 является теорема:

Теорема (2.3.26) Пусть $A \in M_n(0,1)$ и A — вполне неразложимая матрица. Если $\nu(A) < 2n+3$, то матрица A конвертируема.

Также рассмотрен вопрос конвертируемости неразложимых матриц. Построен **пример** (2.3.28), показывающий, что последняя теорема не обобщается на неразложимые матрицы.

В разделе 2.4 рассмотрена операция расширения матрицы.

Определение (2.4.5) Расширением (0,1)-матрицы A по i-тому столбцу будем называть множество матриц $\mathfrak{R}(A)$ такое, что для каждой $B \in \mathfrak{R}(A)$ имеем $B \in M_{n+1}(0,1)$, $b_{1,i} = b_{1,i+1} = 1$ и $\mathfrak{S}(B) = A$.

Операция расширения является удобным инструментом для описания вполне неразложимых неконвертируемых (0,1)-матриц порядка n с $2n+3$ единицами. В частности, имеет место следующее полезное свойство, которое говорит о том, что любую вполне неразложимую неконвертируемую (0,1)-матрицу порядка n с $2n+3$ единицами можно построить как последовательность расширений.

Лемма (2.4.7) Пусть Y — множество вполне неразложимых неконвертируемых (0,1)-матриц порядка n с $(2n+3)$ ненулевыми элементами. Тогда любая вполне неразложимая неконвертируемая матрица A порядка $(n+1)$ с $2(n+1)+3$ элементами перестановочно эквивалентна одной из матриц из множества $\cup_{B\in Y}\mathfrak{R}(B)$, где в объединении берутся расширения по всем столбцам матриц B.

Последняя лемма позволяет описать все вполне неразложимые неконвертируемые (0,1)-матрицы с $(2n+3)$ ненулевыми элементами. Через R_n обозначим матрицу порядка n, определенную по правилу:

$$r_{ij} = \begin{cases} 1, & \text{если } i+j=n \text{ или } i+j=n+1 \\ 0, & \text{иначе.} \end{cases}$$

Определение (2.4.10) Будем говорить, что выполнена операция расширения (0,1)-матрицы A с выбором, если выбрана одна из матриц из множества $\mathfrak{R}(A)$.

Лемма (2.4.11) Пусть дана матрица размера 3 на 1 (вектор-столбец размера 3), заполненная единицами. К этой матрице k раз применили операцию расширения с выбором, и получили матрицу B размера $(k+3)\times(k+1)$. Пусть после каждого шага в каждом столбце полученной матрицы не менее 2 ненулевых элементов. Тогда существуют целые неотрицательные числа k_1, k_2 и k_3, где $k_1+k_2+k_3=k$, и матрицы перестановок P, Q строк и столбцов матрицы B такие, что матрица PBQ имеет следующий вид:

$$T = \begin{pmatrix} V_{k_1} & O_{k_1,k_3} & O_{k_1,k_2} & R_{k_1} \\ V_{k_2} & O_{k_2,k_3} & R_{k_2} & O_{k_2,k_1} \\ V_{k_3} & R_{k_3} & O_{k_3,k_2} & O_{k_3,k_1} \\ W_0 & W_3 & W_2 & W_1 \end{pmatrix} = \begin{pmatrix} \overline{C_k} \\ \overline{W_k} \end{pmatrix} \qquad (0.1)$$

где:

1. V_{k_i} — вектор столбец из k_i элементов с единственным единичным элементом, стоящим на последнем месте, если $k_i > 0$, и пустой вектор, если k_i

$= 0.$

2. W_0 — вектор столбец из трех элементов.

3. В первом столбце матрицы (2.10) три ненулевых элемента.

4. Каждая из подматриц W_i, где $i = 1, 2, 3$, имеет размеры $3 \times k_i$ и при $k_i > 0$ имеет единственный ненулевой элемент, который находится в i-той строке в последнем столбце.

5. В каждой строке подматрицы $\overline{W_k} = \begin{pmatrix} W_0 & W_3 & W_2 & W_1 \end{pmatrix}$ содержится единственный единичный элемент.

В выражение (0.1) матрица разбита на блоки $\overline{W_k}$ и $\overline{C_k}$, где k означает число проделанных операций расширения с выбором, $\overline{W_k}$ включает в себя три последние строки полученной матрицы, а $\overline{C_k}$ включает все строки, кроме 3 последних. Данные блоки лежат в основе описания вполне неразложимые неконвертируемые (0,1)-матрицы с $(2n + 3)$ ненулевыми элементами.

Теорема (2.4.13) Пусть $n \geq 3$. Для любой вполне неразложимой неконвертируемой матрицы $A \in M_n(0, 1)$ с $\nu(A) = 2n + 3$ существуют неотрицательные целые числа m_1, m_2, m_3 такие, что $m_1 + m_2 + m_3 + 3 = n$ и матрица A с точностью до перестановки строк и столбцов имеет вид:

$$\begin{pmatrix} \overline{C_{m_1}} & O_{m_1,m_2+1} & O_{m_1,m_3+1} \\ O_{m_2,m_1+1} & \overline{C_{m_2}} & O_{m_2,m_3+1} \\ O_{m_3,m_1+1} & O_{m_3,m_2+1} & \overline{C_{m_3}} \\ \overline{W_{m_1}} & \overline{W_{m_2}} & \overline{W_{m_3}} \end{pmatrix} \tag{0.2}$$

где $\overline{C_{m_i}}$ и $\overline{W_{m_i}}$ — блоки матрицы T, которая задана формулой (2.10), а $O_{i,j}$ нулевая подматрица порядка $i \times j$.

Глава 3 посвящена изучению перманента матриц над конечным полем.

В разделе 3.2 изучается аналог конвертации для матриц над конечным полем. В случае поля $\mathbb{F}_q$ конечной характеристики понятие конвертации является содержательным при char $(\mathbb{F}_q) \geq 3$. Для минимально возможного поля $\mathbb{F}_3$ из 3 элементов доказано, что любая матрица $A \in M_n(\mathbb{F}_3)$ всегда конвертируема.

Теорема (3.2.11) Пусть $A \in M_n(\mathbb{F}_3)$, тогда существует $X \in M_n(\pm 1)$ такая, что per $(A) =$ det $(A \circ X)$.

Доказано, что поле $\mathbb{F}_3$ является единственным исключением. А именно, для любого другого конечного поля $\mathbb{F}_q$, где char $(\mathbb{F}_q) \geq 3$, существуют примеры неконвертируемых матриц.

Теорема (3.2.14) Для всякого поля $\mathbb{F}_q$, такого, что char $(\mathbb{F}_q) \geq 3$ и $|\mathbb{F}_q| \geq 5$, и для любого $n \geq 3$ существует неконвертируемая матрица $A \in M_n(\mathbb{F}_q)$.

Построена серия примеров, доказывающая невозможность запрета конвертации в терминах количества ненулевых элементов для матриц над конечным полем.

Теорема (3.2.24) Пусть $\mathbb{F}_q$ — поле характеристики $p \geq 3$. Тогда для любого $n \geq (p-1)$ существует конвертируемая матрица с ненулевым перманентом, которая не содержит нулевых элементов.

В случае поля конечной характеристики было доказано несколько достаточных условий конвертируемости матриц, в том числе следующий, не имеющий прямого аналога для неотрицательных матриц.

Теорема (3.2.29) Пусть матрица $A \in M_n(\mathbb{F}_p)$, $p > 2$ и $n \geq 2p - 6$, удовлетворяет следующим условиям:

1. Один из столбцов не содержит нулевых элементов.

2. В одной из строк не менее

$$M = (p-3)\log(n-1)(p-1) + 2$$

ненулевых элементов.

3. Матрица A вполне неразложима.

Тогда матрица A конвертируема.

В разделе 3.3 введено понятие тензора перманента, доказаны его основные свойства.

Определение (3.3.1) Пусть $e_1, \ldots, e_n$ — стандартный базис линейного пространства $V_n = \mathbb{F}_q^n$. Пусть $A \in M_{k \times n}(\mathbb{F}_q)$, где $k < n$. Рассмотрим $(n-k)$-мерный контравариантный тензор $T_A = T_A^{i_1, \ldots, i_{n-k}}$ заданный на пространстве $V_n^{n-k} = \underbrace{V_n \otimes \ldots \otimes V_n}_{n-k \text{ раз}}$. Зададим компоненты тензора в базисе $e_1, \ldots, e_n$ по правилу:

$$T_A^{i_1, \ldots, i_{n-k}} = \begin{cases} \text{per } (A(|i_1, \ldots, i_{n-k})), \text{ если все } i_1, \ldots, i_{n-k} \text{ различны} \\ 0 \text{ в противном случае.} \end{cases}$$

Тензор T_A будем называть тензором перманента матрицы A. В случае, если $k = 1$, матрица может быть рассмотрена как вектор $A \in M_{1,n}(\mathbb{F}_q) = \mathbb{F}_q^n$, и мы будем называть T_A тензором вектора A.

Определение (3.3.4) Пусть $a = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ — вектор с n компонентами. Пусть $A \in M_{k,n}(\mathbb{F}_q)$, T_A обозначает тензор перманента матрицы A. Сверткой тензора T_A и вектора a называется тензор $\overline{T} = T_A \circ a$, компоненты которого заданы по следующему правилу:

$$\overline{T}^{i_1, \ldots, i_{n-k-1}} = \sum_{j=1}^{n} T^{i_1, \ldots, i_{n-k-1}, j} \cdot a_j.$$

Одним из ключевых свойств тензора перманента является следующая теорема.

Теорема (3.3.6) Пусть матрица $A \in M_n(\mathbb{F}_q)$ представлена как набор строк $a_1, \ldots, a_n$. Тогда для перманента матрицы A справедлива формула:

$$\text{per } (A) = (\ldots(T_{a_n} \circ a_{n-1}) \circ a_{n-2} \ldots) \circ a_1.$$

Разработанная техника в разделе 3.4 использована для получения оценки числа матриц с нулевым перманентом в пространстве матриц над конечным полем.

Теорема (3.4.10) Пусть $\mathbb{F}_q$ — конечное поле из q элемент, характеристика которого больше 2. Тогда имеет место неравенство:

$$D(M_n(\mathbb{F}_q)) > P(M_n(\mathbb{F}_q)).$$

Как следствие этой теоремы, доказано несуществование биективного отображения, позволяющего заменить вычисление перманента на вычисление определителя для матриц над конечным полем.

Теорема (3.4.12) Пусть $\mathbb{F}_q$ — конечное поле из q элементов, $\mathrm{char}\,(\mathbb{F}_q) = p \geq 3$, $M_n(\mathbb{F}_q)$ — кольцо квадратных матриц, где $n \geq 3$. Тогда не существует биективного отображения

$$G : M_n(\mathbb{F}_q) \to M_n(\mathbb{F}_q),$$

такого, что $\mathrm{per}\,(A) = \det\,(G(A))$.

В частности, из этого следует, что даже в случае поля $\mathbb{F}_3$ универсальной матрицы $X \in M_n(\pm 1)$, которая бы конвертировала любую матрицу $A \in M_n(\mathbb{F}_3)$ не существует.

Благодарность

Автор выражает глубокую благодарность своему научному руководителю — доктору физико-математических наук, профессору Александру Эмилевичу Гутерману за постановку задачи, постоянное внимание к работе и всестороннюю поддержку, а также всему коллективу кафедры высшей алгебры за доброжелательную и творческую атмосферу.

Глава 1

Знаковая конвертация матриц

1.1 Основные определения и обозначения

1.1.1 Понятие конвертации перманента матрицы

Перманент и определитель квадратной матрицы $A = (a_{ij})$ порядка n над произвольным полем $\mathbb{F}$ определяются следующим образом:

$$\operatorname{per}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i\sigma(i)}; \quad \det(A) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)} \tag{1.1}$$

В выражении (1.1) через S_n обозначена группа перестановок порядка n, а через $\operatorname{sign}(\sigma)$ — знак перестановки σ.

Обозначение 1.1.1. Через $M_{m,n}(X)$ будем обозначать множество прямоугольных матриц из m строк и n столбцов с элементами из множества X. Если $m = n$, то будем использовать сокращенное обозначение $M_{n,n}(X) = M_n(X)$. В качестве X мы рассматриваем поле или какое-либо его подмножество.

Определение 1.1.2. Пусть $A = (a_{ij}) \in M_n(X)$ — квадратная матрица порядка n. Множество элементов $\{a_{1\sigma(1)}, \dots, a_{n\sigma(n)}\}$ будем называть обобщенной диагональю матрицы A, которая соответствует перестановке σ, или просто обобщенной диагональю. Произведение $\prod\limits_{i=1}^{n} a_{i\sigma(i)}$ называется диагональным произведением.

Определение 1.1.3. Обобщенная диагональ матрицы A называется ненулевой (положительной), если соответствующее диагональное произведение не равно нулю (положительно).

Таким образом, перманент матрицы может быть определен как сумма всех диагональных произведений.

Определение 1.1.4. Пусть $A = (a_{ij}), B = (b_{ij}) \in M_n(X)$ — две квадратные матрицы одного порядка n. Адамаровым произведением матриц A и B называется матрица $A \circ B = C = (c_{ij})$ порядка n, полученная поэлементным умножением заданных матриц, то есть $c_{ij} = a_{ij}b_{ij}$ для любых $i, j \in \overline{1, \ldots, n}$.

Используя адамарово произведение матриц, можно сформулировать следующее понятие знаковой конвертации, эквивалентное данному во введении определению.

Определение 1.1.5. Квадратная матрица A порядка n называется знаково конвертируемой, если существует матрица $X \in M_n(\pm 1)$ такая, что выполнено равенство:

$$\mathrm{per}\,(A) = \det\,(A \circ X). \tag{1.2}$$

Замечание 1.1.6. Далее всюду, где не оговорено противное, вместо понятия знаковой конвертации будем говорить просто о конвертации матриц.

Обозначение 1.1.7. Если выполнено тождество (1.2), то будем говорить, что матрица X конвертирует матрицу A.

Проблема 1 может быть переформулирована следующим образом:

Проблема 1.1.8. Когда квадратная матрица A порядка n конвертируема?

1.1.2 Примеры использования функции перманента

Обозначение 1.1.9. Пусть α и β — два набора различных индексов от 1 до n. Через $A(\alpha|\beta)$ будем обозначать матрицу, полученную вычеркиванием из A строк с номерами из α и столбцов с номерами из β. Через $A[\alpha|\beta]$ будем обозначать матрицу, каоторая лежит на пересечении строк с номерами из α и столбцов с номерами из β.

Функция перманента может быть обобщена на прямоугольные матрицы порядка $m \times n$, где $m \leq n$. Это обобщение используется во многих комбинаторных задачах.

Определение 1.1.10. Пусть $A \in M_{m\times n}$, где $m \leq n$, и $k = n - m$. Перманентом матрицы A называется функция

$$\text{per}\,(A) = \sum_{j_1<\ldots<j_k} \text{per}\,(A(|j_1,\ldots,j_k))$$

Классическим является следующий пример использования перманента.

Пример 1.1.11 (Бруалди, Райзер, [13], раздел 7.2)**.** Пусть на фабрике открыто n вакансий и существует n рабочих, каждый из которых умеет работать на каких-то из имеющихся вакансий. Составим матрицу A порядка n, где $a_{ij} = 1$, если i-тый рабочий умеет работать на j-той вакансии, и $a_{ij} = 0$ в противном случае. Тогда перманент матрицы A равен числу различных способов трудоустроить всех рабочих так, чтобы все вакансии оказались занятыми.

Этот пример обобщается до задачи, известной как существование системы различных представителей.

Пример 1.1.12 (Бруалди, Райзер, [13], раздел 7.2)**.** Пусть дано конечное множество X из n элементов и конечная система его подмножеств $X_1, \ldots, X_m$, где $m \leq n$. Множество попарно различных элементов

$(x_{k_1}, \ldots, x_{k_m})$ называется системой различных представителей для подмножеств $X_1, \ldots, X_m$, если $x_{k_i} \in X_i$. Построим прямоугольную матрицу A из m строк и n столбцов, где $a_{ij} = 1$ если в i-том множестве лежит j-тый элемент и $a_{ij} = 0$ в противном случае. Число систем различных представителей для подмножеств $X_1, \ldots, X_m$ равно перманенту матрицы A.

Пример 1.1.13 (Бруалди, Райзер, [13], раздел 7.2)**.** Задача о подсчете числа беспорядков D_n . Беспорядком называется перестановка $\sigma \in S_n$ такая, что $\sigma(i) \neq i$ для любого значения i. Решение этой задачи может быть сведено к вычислению перманента матрицы

$$\begin{pmatrix} 0 & 1 & \ldots & 1 \\ 1 & 0 & \ldots & 1 \\ \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & \ldots & 0 \end{pmatrix}.$$

Действительно. Обобщенная диагональ построенной матрицы будет ненулевой тогда и только тогда, когда ни один из ее элементов не лежит на главной диагонали. Это равносильно тому, что этой обобщенной диагонали соответствует перестановка $\sigma \in S_n$ такая, что $\sigma(i) \neq i$ для любого значения i. Вычисляя перманент последней матрицы, можно найти значение D_n:

$$D_n = \sum_{r=0}^{n-1} (-1)^r C_n^r (n-r)^{n-r} (n-r-1)^{n-r},$$

где C_n^r обозначает соответствующий биномиальный коэффициент.

Пример 1.1.14 (Бруалди, Райзер, [13], раздел 7.2)**.** Эта задача известна как задача о рассадке гостей. Пусть необходимо посадить n женатых пар за круглым столом так, чтобы мужчины и женщины чередовались и никакая женатая пара не сидела рядом друг с другом. Обозначим искомое число через U_n. Вначале можно произвольно рассадить жен, существует всего $2(n!)$ способов это сделать. После этого, если жена сидит на i-том месте, то муж не может сидеть на i-том и $(i+1)$-ом местах. Таким образом, число U_n можно найти в виде

$$U_n = 2(n!)K_n,$$

где K_n равно числу таких $\sigma \in S_n$, что $\sigma(i) \neq i$ и $\sigma(i) \neq (i+1)$. Число K_n может быть вычислено как перманент матрицы следующего вида:

$$\begin{pmatrix} 0 & 0 & 1 & \dots & 1 & 1 \\ 1 & 0 & 0 & \dots & 1 & 1 \\ 1 & 1 & 0 & \dots & 1 & 1 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & \dots & 0 & 0 \\ 0 & 1 & 1 & \dots & 1 & 0 \end{pmatrix}$$

Для перманента последней матрицы имеет место следующая формула:

$$K_n = \sum_{k=0}^{n} (-1)^k \frac{2n}{2n-k} C_{2n-k}^{k} (n-k)!.$$

1.2 Примеры конвертируемых и неконвертируемых матриц

Понятие конвертируемости матрицы является содержательным при $n \geq 3$. То есть, существуют, как конвертируемые, так и неконвертируемые матрицы порядка $n \geq 3$.

Пример 1.2.1 (Полиа, [36]). Матрица порядка 2 всегда конвертируемая. Более того, конвертация осуществляется с помощью одной и той же матрицы X. Пусть

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \text{ и } X = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix},$$

тогда имеет место равенство:

$$\operatorname{per}(A) = a_{11}a_{22} + a_{12}a_{21} = \det \begin{pmatrix} a_{11} & -a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \det(A \circ X)$$

Пример 1.2.2. Матрица

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

конвертируема. Имеет место равенство:

$$\operatorname{per} \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = \det \begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & -1 \\ 1 & 1 & 1 \end{pmatrix}$$

Обозначение 1.2.3. Через I_n будем обозначать единичную матрицу порядка n. Через J_n будем обозначать матрицу порядка n, состоящую из единичных элементов.

Пример 1.2.4. Матрица

$$A = J_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

неконвертируема. Так как $\operatorname{per}(A) = 6$, а определитель матрицы $X \in M_3(\pm 1)$ не может быть равен 6, то для любой $X \in M_3(\pm 1)$ имеем неравенство $\operatorname{per}(A) \neq \det(X) = \det(A \circ X)$.

Последний пример может быть обобщен для получения неконвертируемой матрицы любого порядка $n \geq 3$.

Пример 1.2.5. Для любого $n \geq 3$ существует неконвертируемая матрица $A \in M_n(0,1)$, определенная как прямая сумма $A = I_{n-3} \oplus J_3$.

Следующая теорема дает целую серию примеров неконвертируемых матриц:

Теорема 1.2.6 (Гибсон, [22]). Пусть $A \in M_n(0,1)$ — конвертируемая матрица и per $(A) > 0$. Тогда в матрице A не более, чем $\Omega_n = \frac{n^2+3n-2}{2}$ единичных элементов. Более того, если число единичных элементов в точности равно Ω_n, то существуют матрицы перестановок P и Q такие, что

$$PAQ = G_n = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ 1 & 1 & 1 & 0 & \dots & 0 & 0 \\ 1 & 1 & 1 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & 1 & \dots & 1 & 0 \\ 1 & 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & 1 & 1 & 1 & \dots & 1 & 1 \end{pmatrix} \tag{1.3}$$

Существуют и исключительные случаи, в которых понятие конвертации не является содержательным.

Пример 1.2.7. Для любой матрицы $A \in M_n(\mathbb{F}_q)$, где характеристика поля char $\mathbb{F}_q = 2$, имеет место равенство per $(A) =$ det (A). Действительно, если характеристика поля равна 2, то $1 = -1$, а значит определитель матрицы равен перманенту, а умножение элементов на -1 не изменяет матрицу.

1.3 Свойство конвертируемости и арифметические операции на матрицах

1.3.1 Конвертируемость суммы матриц

Обозначение 1.3.1. Пусть A — неотрицательная матрица. Через $\phi(A)$ обозначим матрицу, полученную из A заменой всех ненулевых элементов на единицы.

Определение 1.3.2. Пусть $A \in M_n(\mathbb{R})$ — вещественная матрица. Знаковой схемой матрицы A называется матрица $\mathrm{sign}(A)$ полученная заменой всех положительных элементов на 1 и всех отрицательных элементов на -1.

Определение 1.3.3. Матрица $A \in M_n(0, \pm 1)$ называется знаково невырожденной, если любая вещественная матрица с такой же знаковой схемой невырождена.

Теорема 1.3.4 (Бруалди, Шейдер, [14])**.** Невырожденная вещественная матрица A знаково невырождена тогда и только тогда, когда все диагональные произведения матрицы A, умноженные на знак соответствующей перестановки, неотрицательны(неположительны), и существует как минимум одно ненулевое диагональное произведение.

Для вещественной матрицы $A = (a_{ij})$ через $|A|$ обозначим матрицу вида $(|a_{ij}|)$.

Теорема 1.3.5 (Бруалди, Шейдер, [14])**.** Пусть $A \in M_n(\mathbb{R})$. Тогда матрица A знаково невырождена в том и только в том случае, когда $\mathrm{per}\ (|A|) = |\det\ (A)|$.

Следствие 1.3.6. Неотрицательная матрица A конвертируема тогда и только тогда, когда конвертируема матрица $\phi(A)$.

Доказательство. Если per $(A) = 0$, то все диагональные произведения в A равны нулю и per $(A) = 0 =$ det (A). Это свойство очевидно сохраняется при замене положительных элементов матрицы A на единицы. Следовательно per $(\phi(A)) = 0 =$ det $(\phi(A))$.

Пусть per $(A) > 0$. Если неотрицательная матрица A конвертируема, то существует матрица $X \in M_n(\pm 1)$ такая, что имеет место равенство per $(A) =$ det $(A \circ X) > 0$. Очевидно, что $|A \circ X| = A$. Получаем равенство per $(|A \circ X|) = |$det $(A \circ X)|$. По теореме 1.3.5 матрица $A \circ X$ знаково невырождена. Так как det $(A \circ X) > 0$, то по теореме 1.3.4 все диагональные произведения матрицы $A \circ X$, умноженные на знак перестановки, неотрицательны. Таким образом, в перманент A и определитель $A \circ X$ входят одни и те же диагональные произведения с одинаковыми знаками. Очевидно, что это свойство сохраняется при замене положительных элементов в A на другие положительные элементы, что доказывает нашу лемму. □

Следствие 1.3.7. Пусть $A, B \in M_n(0, 1)$ и матрица A конвертируется матрицей $X \in M_n(\pm 1)$. Тогда матрица $A \circ B$ конвертируется матрицей X.

Доказательство. Если per $(A) = 0$, то в матрице A нет ненулевых диагональных произведений. При умножении $A \circ B$ в матрице не появиться новых ненулевых элементов, а значит все диагональные произведения для матрицы $A \circ B$ будут нулевыми. Получаем равенство per $(A \circ B) = 0 =$ det $(A \circ B \circ X)$.

Пусть per $(A) > 0$. Так как матрица A конвертируется матрицей X, то по теореме 1.3.5 матрица $A \circ X$ знаково невырождена. Так как det $(A \circ X) =$ per $(A) = 0$, то по теореме 1.3.4 все диагональные произведения матрицы $A \circ X$, умноженные на знак перестановки, неотрицательны. Так как B — неотрицательная матрица, то все диагональные произведения матрицы $A \circ X \circ B$, умноженные на знак перестановки, неотрицательны. В силу неотрицательности матрицы $A \circ B$ получаем равенство per $(A \circ B) = \det (A \circ B \circ X)$. Таким образом, матрица $A \circ B$ конвертируема с помощью матрицы X. Следствие доказано. □

Следствие 1.3.8. Пусть A — неотрицательная матрица. Тогда для любой $X \in M_n(\pm 1)$ имеет место неравенство per $(A) \geq |\det (A \circ X)|$. Равенство возможно только для конвертируемой матрицы A.

Доказательство. При вычислении перманента неотрицательной матрицы все диагональные произведения неотрицательны. При вычислении определителя матрицы $A \circ X$ диагональные произведения, умноженные на знак перестановки, имеют тот же модуль, что и для перманента матрицы A, но могут иметь разные знаки. Таким образом, получили требуемое неравенство.

Неравенство per $(A) \geq |\det (A \circ X)|$ обращается в равенство только в том случае, если при вычислении определителя матрицы $A \circ X$ диагональные произведения, умноженные на знак соответствующей перестановки, имеют один знак. Раскроем модуль. Если per $(A) = \det (A \circ X)$, то матрица A конвертируема. Пусть per $(A) = -\det (A \circ X)$. Возьмем матрицу X', которая отличается от матрицы X умножением первой строки на минус один. Получаем равенство per $(A) = \det (A \circ X')$. Следовательно, матрица A конвертируема. Следствие доказано. □

Следствие 1.3.9. Пусть A — неотрицательная блочная верхнетреугольная матрица с диагональными блоками $A_1, \ldots, A_k$ и per $(A) > 0$. Тогда имеют место следующие утверждения:

1. Если подматрицы $A_1, \ldots, A_k$ конвертируемые, то матрица A конвертируемая.

2. Если подматрицы $A_1, \dots, A_k$ неконвертируемые, то матрица A неконвертируемая.

Доказательство. В силу формулы Лапласа для перманента имеет место равенство: $\mathrm{per}\ (A) = \mathrm{per}\ (A_1)\mathrm{per}\ (A_2) \dots \mathrm{per}\ (A_k)$. Если каждая из подматриц A_i конвертируется с помощью матрицы X_i, то выберем матрицу $X \in M_n(\pm 1)$, где блоки X_i стоят на главной диагонали. Получаем равенства:

$$\mathrm{per}\ (A) = \prod_{i=1}^{k} \mathrm{per}\ (A_i) = \prod_{i=1}^{k} \det\ (A_i \circ X_i) = \det\ (A \circ X).$$

Таким образом, матрица A конвертируема.

Пусть каждый из блоков A_i неконвертируем. Тогда по следствию 1.3.8 для любой матрицы $X \in M_n(\pm 1)$ с блоками X_i на главной диагонали такими, что размеры X_i совпадают с размерами A_i, получаем $\mathrm{per}\ (A_i) > |\det\ (A_i \circ X_i)|$. Таким образом, верно неравенство:

$$\mathrm{per}\ (A) = \prod_{i=1}^{k} \mathrm{per}\ (A_i) > \prod_{i=1}^{k} |\det\ (A_i \circ X_i)| = |\det\ (A \circ X)|.$$

Так как последнее неравенство верно для произвольной матрицы $X \in M_n(\pm 1)$, то матрица A неконвертируема. Следствие доказано. □

В общем случае сумма неотрицательных матриц может быть, как конвертируемой, так и неконвертируемой матрицей.

Пример 1.3.10. Пусть

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Матрицы A, B конвертируемы, так как $\mathrm{per}\ (A) = \det\ (A)$ и $\mathrm{per}\ (B) = \det\ (B)$. Матрица $J_3 = (A + B)$ неконвертируема (см. пример 1.2.4).

Пример 1.3.11. Пусть A — конвертируемая неотрицательная матрица. Тогда матрица $(A + A)$ конвертируема. Действительно, $\phi(A + A) = \phi(A)$. По следствию 1.3.6 матрица $(A + A)$ конвертируема.

Обозначение 1.3.12. Пусть A, B — неотрицательные матрицы. Будем говорить, что $A \leq B$, если $a_{ij} \leq b_{ij}$ для любой допустимой пары индексов.

Теорема 1.3.13. Пусть A, B — вещественные неотрицательные квадратные матрицы с положительным перманентом. Тогда матрица $(A+B)$ конвертируема в том и только в том случае, когда существует конвертируемая матрица $C \in M_n(0, 1)$ такая, что $\phi(A) \leq C$ и $\phi(B) \leq C$.

ДОКАЗАТЕЛЬСТВО. Если существует конвертируемая матрица $C \in M_n(0, 1)$ такая, что $\phi(A) \leq C$ и $\phi(B) \leq C$, то в силу неотрицательности матриц A, B, имеем $\phi(A + B) \leq C$. Это означает, что существует матрица $D \in M_n(0, 1)$ такая, что $\phi(A+B) = (C \circ D)$. По следствию 1.3.7 матрица $C \circ D$ конвертируема, а значит по следствию 1.3.6 матрица $(A + B)$ конвертируема.

Докажем обратное. Пусть матрица $(A+B)$ конвертируема. Тогда положим $C = \phi(A + B)$. Тогда матрица C конвертируема по следствию 1.3.6, а из неотрицательности матриц A, B получаем неравенства $\phi(A) \leq C$ и $\phi(B) \leq C$. Что и требовалось доказать. □

Следствие 1.3.14. Пусть A, B — неотрицательные матрицы и матрица A неконвертируема. Тогда матрица $(A + B)$ неконвертируема.

1.3.2 Максимальные конвертируемые матрицы и знаковая конвертируемость при матричном умножении

Произведение конвертируемых матриц может быть, как конвертируемой, так и неконвертируемой матрицей.

Пример 1.3.15. Матрица

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

конвертируема:

$$\operatorname{per} \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = 4 = \det \begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & -1 \\ 1 & 1 & 1 \end{pmatrix}$$

При этом матрица A^2:

$$A^2 = \begin{pmatrix} 2 & 2 & 1 \\ 3 & 3 & 2 \\ 3 & 3 & 2 \end{pmatrix}$$

неконвертируема. Действительно, по следствию 1.3.6 матрица A^2 конвертируема тогда и только тогда, когда конвертируема матрица $\phi(A^2) = J_3$. В примере 1.2.4 было показано, что матрица J_3 неконвертируема.

Пример 1.3.16. Пусть A — конвертируемая (0,1)-матрица. Умножение A на матрицу перестановки дает конвертируемую матрицу.

Как видно из примера 1.3.15 в общем случае сказать что-либо о конвертируемости произведения неотрицательных матриц нельзя. Поэтому мы рассмотрим следующее подмножество (0,1)-матриц.

Определение 1.3.17. Максимальной конвертируемой матрицей называется конвертируемая (0,1)-матрица, в которой замена любого нулевого элемента на единицу дает неконвертируемую матрицу.

Для максимальных конвертируемых матриц удается доказать необходимое условие конвертируемости произведения AB, где одна из матриц максимальная конвертируемая, а вторая неотрицательная. Для начала докажем следующую вспомогательную лемму.

Лемма 1.3.18. Пусть $A \in M_n(0,1)$ — квадратная матрица и $\alpha = (i_1, \ldots, i_k), \beta = (j_1, \ldots, j_k)$, где $1 \le i_1 < i_2 < \ldots < i_k \le n$ и $1 \le j_1 < \ldots < j_k \le n$, — два набора различных индексов, для которых верны следующие утверждения:

1. $A(\alpha|\beta)$ — неконвертируемая матрица
2. $\text{per}\,(A[\alpha|\beta]) > 0$.

Тогда матрица A неконвертируема.

Доказательство. Предположим, что матрица A конвертируема. Так как при перестановке строк и столбцов конвертируемость матрицы сохраняется, то можно считать, что $\alpha = \beta = (1, \ldots, k)$.

Выберем матрицу $B \in M_n(0,1)$ такую, что $(A \circ B)$ примет блочно-диагональный вид с блоками $A(\alpha|\alpha)$ и $A[\alpha|\alpha]$. Так как $A(\alpha|\alpha)$ неконвертируема, то в ней существуют ненулевые обобщенные диагонали. Следовательно, $\text{per}\,(A(\alpha|\alpha)) > 0$. Имеет место неравенство

$$\text{per}\,(A \circ B) = \text{per}\,(A[\alpha|\alpha])\text{per}\,(A(\alpha|\alpha)) > 0 \tag{1.4}$$

В силу сделанного предположения о конвертируемости матрицы A по следствию 1.3.7 матрица $(A \circ B)$ конвертируема. Из равенства (1.4) и следствия 1.3.8 получаем, что матрица $A \circ B$ конвертируема тогда и только тогда, когда конвертируем каждый из блоков. Это противоречит первому условию леммы. Таким образом, матрица A неконвертируема. □

Обозначение 1.3.19. Через $U_{m,n} \in M_n(0,1)$ обозначим матрицу следующего вида:

$$u_{ij} = \begin{cases} 1, & \text{если } 2 \leq j = i+1 \leq m \\ 1, & \text{если } i = m, j = 1 \\ 0, & \text{иначе.} \end{cases} \tag{1.5}$$

Теорема 1.3.20. Пусть A, B — неотрицательные матрицы, где A — максимальная конвертируемая матрица с положительным перманентом и $\phi(B) \geq (U_{m,n} + I_n), m \geq 3$. Тогда матрицы BA и AB неконвертируемы.

Доказательство. Начнем со случая произведения BA. Доказательство проведем от противного. Предположим, что матрица BA конвертируема.

Замена некоторых внедиагональных ненулевых элементов матрицы B на нулевые может только уменьшить число ненулевых элементов в произведении BA, а значит существует матрица $X \in M_n(0,1)$ такая, что $\phi(X \circ (BA)) = \phi((U_{m,n} + I_n)A)$. По следствию 1.3.7 матрица $(U_{m,n} + I_n)A$ конвертируема.

Раскрывая скобки, получаем $(U_{m,n} + I_n)A = A + A'$, где A' получена из A циклической перестановкой первых m строк с помощью перестановки $\sigma = (1, \ldots, m)^{-1}$ и заменой всех остальных строк нулевыми. Таким образом, выполнено неравенство:

$$\phi((U_{m,n} + I_n)A) \geq \phi(A) \tag{1.6}$$

Так как A — максимальная конвертируемая матрица, и, по сделанному предположению, матрица $(U_{m,n} + I_n)A$ тоже конвертируема, то в (1.6) имеет место строгое равенство. В силу неотрицательности матрицы A из (1.6) следует неравенство:

$$\phi(U_{m,n}A) \leq \phi(A). \tag{1.7}$$

В неравенстве (1.7) рассмотрим только первые m строк матриц. Из определения матрицы $U_{m,n}$ получаем цепочку неравенств:

$$\phi(a_1) \geq \phi(a_2) \geq \ldots \geq \phi(a_m) \geq \phi(a_1), \tag{1.8}$$

здесь $a_1, \ldots, a_m$ — первые m векторов строк матрицы A.

Получаем, что в (1.8) имеют место равенства.

Таким образом, первые m строк можно разбить на две подматрицы. Первая из этих подматриц $A[1, \ldots, m|i_1, \ldots, i_k]$ не содержит нулевых элементов. Вторая подматрица $A[1, \ldots, m|j_1, \ldots, j_{n-k}]$, где $\{i_1, \ldots, i_k\} \cup \{j_1, \ldots, j_{n-k}\} = \{1, \ldots, n\}$ и $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_{n-k}\} = \emptyset$, является нулевой.

В матрице существует обобщенная диагональ $\{a_{1,\sigma(1)}, \ldots, a_{n,\sigma(n)}\}$ из ненулевых элементов. В силу общего вида матрицы, подматрица $D = A[1, \ldots, m|\sigma(1), \ldots, \sigma(m)]$ не содержит нулевых элементов. По следствию 1.3.6 подматрица D конвертируема тогда и только тогда, когда конвертируема матрица $J_m = \phi(D)$. По теореме 2 матрица J_m неконвертируема при $m \geq 3$. Таким образом, подматрица D неконвертируема. Кроме того, в силу существования указанной обобщенной диагонали и неотрицательности матрицы A, имеет место неравенство

$$\text{per}\,(A(1, \ldots, m|\sigma(1), \ldots, \sigma(m))) > 0.$$

Таким образом, если $\alpha = \{1, \ldots, m\}$ и $\beta = \{\sigma(1), \ldots, \sigma(m)\}$, то по лемме 1.3.18 матрица A неконвертируема. Это противоречит условию леммы. Таким образом, сделанное предположение неверно и матрица BA неконвертируемая.

Для доказательства леммы относительно произведения AB достаточно заменить перестановку строк на перестановку столбцов. □

Следствие 1.3.21. Пусть A, B — неотрицательные матрицы, где A — максимальная конвертируемая матрица, и существуют матрицы перестановок

P, Q такие, что $\phi(B) \geq P(U_{m,n} + I_n)Q$, $m \geq 3$. Тогда матрицы BA и AB неконвертируемы.

Замечание 1.3.22. Условие $m \geq 3$ существенно. В случае $m = 2$ имеем $\phi(G_n^t(U_{2,n} + I_n)) = \phi(G_n^t) = G_n^t$. В силу теоремы 1.2.6 матрица G_n является максимальной конвертируемой матрицей, а произведение конвертируемо в силу конвертируемости матрицы Гибсона и следствия 1.3.6.

Замечание 1.3.23. Условие $\phi(B) \geq (U_{m,n} + I_n)$, $m \geq 3$, нельзя заменить более слабым требованием существования двух обобщенных диагоналей пересекающихся не более чем по $(n-3)$ элементам. Действительно, выберем в качестве матриц следующие:

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Матрица A конвертируема:

$$\mathrm{per}\,(A) = 8 = \det \begin{pmatrix} 0 & 1 & 1 & -1 \\ 0 & 1 & 1 & 1 \\ 1 & -1 & 1 & 0 \\ 1 & 1 & -1 & 0 \end{pmatrix},$$

а в матрице B существуют две обобщенные ненулевые диагонали, не имеющие общих элементов. При этом BA — конвертируемая матрица:

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 \\ 2 & 2 & 2 & 0 \\ 2 & 2 & 2 & 0 \end{pmatrix}.$$

Матрица BA конвертируема, так как $\phi(BA) = A$, а матрица A конвертируема.

Замечание 1.3.24. Свойство конвертируемости произведения матриц не всегда сохраняется при коммутировании сомножителей. Возьмем матрицы из предыдущего замечания:

$$AB = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 & 2 \\ 1 & 1 & 2 & 2 \\ 2 & 2 & 1 & 1 \\ 2 & 2 & 1 & 1 \end{pmatrix}.$$

По следствию 1.3.6 матрица AB конвертируема тогда и только тогда, когда конвертируема матрица $\phi(AB) = J_4$. По теореме 1.2.6 матрица J_4 неконвертируемая, а значит неконвертируемая и матрица AB.

Теорема 1.3.25. Пусть A — неотрицательная неконвертируемая матрица, а B — неотрицательная матрица такая, что $\mathrm{per}\,(B) > 0$. Тогда матрицы AB и BA неконвертируемы.

Доказательство. Так как $\mathrm{per}\,(B) > 0$ то существует ненулевая обобщенная диагональ. Без ограничения общности можно считать, что она совпадает с главной. Предположим, что матрица AB конвертируема. Тогда по следствию 1.3.6 конвертируема матрица $\phi(AB)$. Далее, имеем:

$$\begin{gathered} \phi(AB) = \phi(\phi(A)\phi(B)) = \phi(\phi(A)(\phi(B) \circ (J - I + I))) = \\ \phi(\phi(A)(\phi(B) \circ (J - I)) + \phi(A)) \qquad (1.9) \end{gathered}$$

В правой части (1.9) написаны две (0,1)-матрицы. По условию матрица A неконвертируема, а значит по следствию 1.3.6 матрица $\phi(A)$ неконвертируема. По следствию 1.3.14 правая часть равенства (1.9) неконвертируема, а значит матрица $\phi(AB)$ неконвертируема. По следствию 1.3.6 неконвертируема и матрица AB.

Неконвертируемость матрицы BA доказывается аналогично. $\square$

1.4 Кронекерово произведение матриц

1.4.1 Связь конвертируемости матрицы с теорией графов

Приведем формулировки результатов из теории графов, которые потребуются для доказательства критерия конвертируемости кронекерова произведения матриц.

Обозначение 1.4.1. Под графом подразумевается простой неориентированный граф без петель и кратных ребер.

Определение 1.4.2. Подмножество M ребер графа G называется паросочетанием, если каждая вершина графа инцидентна не более чем одному ребру из M. Если каждая вершина графа G инцидентна строго одному ребру из M, то паросочетание называется полным.

Обозначение 1.4.3. Через $V(G)$ и $E(G)$ будем обозначать множество вершин и ребер в графе G.

Определение 1.4.4. Граф G называется двудольным, если множество его вершин V можно разделить на два непересекающихся подмножества V_1 и V_2 такие, что никакие две вершины из одного подмножества не инцидентны одному ребру. Множества V_1 и V_2 называются долями графа G.

Обозначение 1.4.5. Пусть G — двудольный граф и $V(G) = V_1 \cup V_2$, где V_1 и V_2 — доли графа G такие, что $|V_1| = m, |V_2| = n$. Тогда графу G можно сопоставить матрицу $A \in M_{m\times n}(0,1)$ такую, что $a_{ij} = 1$ тогда и только тогда, когда существует ребро, которое соединяет i-тую вершину из V_1 с j-той вершиной из V_2. Будем говорить, что матрица A ассоциирована с графом G.

Обозначение 1.4.6. Через $K_{m,n}$ будем обозначать полный двудольный граф с m и n вершинами в долях V_1 и V_2 соответственно.

Определение 1.4.7. Граф G будем называть k-расширяемым, где $k \geq 0$, если любое паросочетание из k ребер можно дополнить до полного паросочетания.

Определение 1.4.8. Подграф H графа G называется центральным, если подграф $G \setminus V(H)$ обладает полным паросочетанием.

Определение 1.4.9. Пусть D — некоторая ориентация графа G. Цикл C называется нечетно ориентированным, если количество ребер, ориентированных в каждую сторону прохождения цикла, нечетно.

Определение 1.4.10. Ориентация D графа G называется пфаффиановой, если каждый центральный цикл в G четной длины нечетно ориентирован.

Теорема 1.4.11 (Литтл, [26]). Пусть $A \in M_n(0, 1)$ и G — ассоциированный с ней двудольный граф. Тогда матрица A конвертируема в том и только том случае, когда существует пфаффианова ориентация графа G.

Теорема 1.4.12 (Робертсон, Сеймор, Томас, [37], теорема 7.3). Каждый 2-расширяемый граф с $n \geq 3$ вершинами и более чем $2n - 4$ ребрами содержит подграф $K_{3,3}$ и, как следствие, не имеет пфаффиановой ориентации.

1.4.2 Критерий конвертируемости кронекерова произведения неотрицательных матриц

Определение 1.4.13. Пусть $A = (a_{ij}) \in M_n$ и $B = (b_{kl}) \in M_m$. Кронекеровым произведением матриц $A \otimes B$ называется блочная матрица порядка mn вида:

$$A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \dots & \dots & \dots \\ a_{n1}B & \dots & a_{nn}B \end{pmatrix}.$$

Лемма 1.4.14. Пусть $A = (a_{ij}) \in M_n$ и $B = (b_{kl}) \in M_m$. Матрицы $A \otimes B$ и $B \otimes A$ перестановочно эквивалентны.

Доказательство. Матрицы $A \otimes B$ и $B \otimes A$ имеют одинаковый порядок mn. Переставим в матрице $A \otimes B$ столбцы таким образом, что каждый столбец с номером $(1+k+ml)$ попадет на $(1+l+kn)$-ое место, где $0 \leq k \leq (m-1)$ и $0 \leq l \leq (n-1)$. В силу выбранного диапазона значения для параметров k, l величины $(1+k+ml)$ и $(1+l+kn)$ принимают все значения от 1 до mn строго по одному разу, а значит это действительно перестановка столбцов. В получившейся матрице строка с номером $(1+k+ml)$ имеет вид $(b_{1,k+1}a_l, b_{2,k+1}a_l, \dots, b_{n,k+1}a_l)$, где a_l строка с номером l из матрицы A. Повторяя для строк полученной матрицы перестановку, примененную к столбцам, получаем матрицу $B \otimes A$, что и требовалось доказать. □

Лемма 1.4.15. Матрица $A \in M_n(0,1)$ содержит единственную ненулевую обобщенную диагональ тогда и только тогда, когда перестановкой строк и столбцов она может быть приведена к верхнетреугольному виду без нулевых элементов на главной диагонали.

Доказательство. Если матрица перестановкой строк и столбцов может быть приведена к верхнетреугольному виду без нулевых элементов на главной диагонали, то, очевидно, содержит единственную ненулевую обобщенную диагональ.

Докажем обратное. Без ограничения общности, можно считать, что ненулевая обобщенная диагональ совпадает с главной диагональю:

$$a_{ii} = 1 \text{ для } i = \overline{1, \dots, n}.$$

Пусть существует $a_{ij} \neq 0$ для $i \neq j$. Если такого элемента нет, то матрица диагональная и все доказано. Так как в матрице A существует единственная обобщенная диагональ, то $\mathrm{per}\ (A(i|j)) = 0$, иначе получаем противоречивое неравенство:

$$1 = \mathrm{per}\ (A) \geq a_{11} \dots a_{nn} + a_{ij} \mathrm{per}\ (A(1|j)) > 1.$$

В последнем неравенстве воспользовались формулой Лапласа разложения по строке и неотрицательностью элементов матрицы.

По теореме Фробениуса-Кенига [7, теорема 2.1] в подматрице $A(i|j)$ есть нулевая подматрица $k \times l$, где $(k + l) \geq n$. Это означает, что исходная матрица A с помощью перестановки строк и столбцов может быть приведена к блочному верхнетреугольному виду с размерами блоков k и l соответственно. Далее повторяем рассуждения для каждого диагонального блока, размер которого больше единицы. На каждом шаге число диагональных блоков увеличивается минимум на один, а значит процесс оборвется не более чем через $(n - 1)$ шаг, и матрица будет верхнетреугольной. □

Лемма 1.4.16. Пусть $A = (I_n + U_{n,n}) \in M_n(0, 1)$ и $B = (I_m + U_{m,m}) \in M_m(0, 1)$, где $m, n > 1$, а матрицы $U_{m,m}$ и $U_{n,n}$ определены выражением (1.5). Тогда матрица $C = A \otimes B$ неконвертируема.

Доказательство. По теореме 1.4.11 для доказательства неконвертируемости матрицы C достаточно доказать невозможность построения пфаффиановой ориентации ассоциированного с матрицей C графа G.

Матрица C порядка mn в каждой строке содержит ровно по 4 ненулевых элемента, так как в каждой строке матриц A и B по 2 ненулевых элемента. Общее количество ребер в графе G равняется $4mn$. Количество вершин в ассоциированном двудольном графе равняется удвоенному порядку матрицы — $2mn$. Для доказательства леммы воспользуемся теоремой 1.4.12. Так как при $m, n > 1$ имеем $4mn > 4mn - 4$, то выполнено условие теоремы 1.4.12 о соотношении числа вершин и ребер графа. Остается доказать, что граф G будет 2-расширяемым.

Предположим противное. Пусть граф G не является 2-расширяемым. Это означает, что можно выбрать какие-то два не смежных ребра из G таким образом, что полученный из G удалением выбранных ребер и всех смежных с ними вершин и ребер граф G_0 не будет содержать полного паросочетания. С точки зрения матриц это означает, что существуют два ненулевых элемента c_{ij}, c_{kl}, лежащих в разных столбцах и строках таких, что per $(C(ik|jl)) = 0$. По теореме Фробениуса-Кенига в матрице $C(ik|jl)$, а значит и в матрице C, существует подматрица размера $l \times k$, где $(l + k) \geq (mn - 1)$, состоящая из нулевых элементов.

Пусть указанная нулевая подматрица расположена на пересечении строк с номерами $i_1, \ldots, i_l$ и столбцов с номерами $j_1, \ldots, j_k$. Далее в доказательстве значения номеров строк и столбцов лежат в интервале $[1, mn]$, и под номером $mn + u$, где $u > 0$, подразумевается столбец с номером u. В силу построения матрицы A имеют место следующие утверждения:

1. Так как по построению матрицы C ее главная диагональ заполнена единичными элементами, то среди столбцов не могут быть столбцы с номерами $i_1, \ldots, i_l$.

2. Так как по построению матрицы C ее обобщенная диагональ, соответствующая перестановке $\sigma = (1, \ldots, mn)$, заполнена ненулевыми элементами, то среди столбцов, входящих в нулевую подматрицу, не могут быть столбцы с номерами $i_1 + 1, \ldots, i_l + 1$.

3. В каждой строке и в каждом столбце матрицы C в точности 4 ненулевых элемента, а значит $l \leq (mn - 4)$ и $k \leq (mn - 4)$.

Рассмотрим два случая.

а) Если среди чисел $i_1, \ldots, i_l$ не все числа идут подряд, то в силу пункта 3 среди чисел $i_1, \ldots, i_l, i_1 + 1, \ldots, i_l + 1$ не менее $(l + 2)$ различных индексов. Это означает, что в матрице C не менее $(k + l + 2) > mn$ столбцов, что неверно, а значит граф G 2-расширяем, и по теореме 1.4.12 для него не существует пфаффиановой ориентации. Таким образом, матрица C неконвертируема.

б) Пусть числа $i_1, \ldots, i_l$ идут подряд. Так как $k \leq (mn - 4)$ и $(k + l) \geq (mn - 1)$ получаем, что $l \geq 3$. По построению матрицы C элементы $c_{i_1, i_1+m}, \ldots, c_{i_l, i_l+m}$ ненулевые, а значит столбцы с номерами $i_1 + m, \ldots, i_l + m$ не могут входить в нулевую подматрицу. Таким образом, выполнены утверждения:

1. $3 \leq l \leq mn - 4$.

2. Столбцы с подряд идущими номерами $i_1, \ldots, i_l$ не могут входить в нулевую подматрицу.

3. Столбцы с подряд идущими номерами $i_1 + m, \ldots, i_l + m$ не могут входить в нулевую подматрицу.

Из этого следует, что среди перечисленных столбцов не менее $(l + 2)$ различных, а значит всего столбцов в матрице не менее $(k + l + 2) \geq mn + 1$, что неверно. Таким образом, граф G — 2-расширяемый. По теореме 1.4.12 для графа G не существует пфаффиановой ориентации, и матрица C неконвертируема. $\square$

Перейдем к доказательству основного результата этой части.

Теорема 1.4.17. Пусть $A \in M_n(0,1)$ и $B \in M_m(0,1)$, и перманенты матриц A и B отличны от нуля. Тогда кронекерово произведение $A \otimes B$ конвертируемо в том и только в том случае, когда одна из матриц содержит единственную обобщенную диагональ без нулевых элементов, а вторая матрица конвертируема.

Доказательство. Пусть одна из матриц содержит единственную обобщенную диагональ без нулевых элементов, а вторая матрица конвертируема. По лемме 1.4.14 матрицы $A \otimes B$ и $B \otimes A$ перестановочно эквивалентны, а значит матрица $A \otimes B$ конвертируема тогда и только тогда, когда конвертируема матрица $B \otimes A$. Таким образом, достаточно рассмотреть случай конвертируемости матрицы $A \otimes B$, где матрица A содержит единственную обобщенную диагональ без нулевых элементов, а матрица B конвертируемая.

Перестановка строк и столбцов в матрице A приводит к перестановке блоков в матрице $A \otimes B$, а значит сохраняет конвертируемость. Таким образом, по лемме 1.4.15 матрицу A можно заменить на верхнетреугольную. Кронекерово произведение матриц $A \otimes B$ будет блочной верхнетреугольной матрицей, где все диагональные блоки равны матрице B. Так как матрица B конвертируема, то блоки на диагонали матрицы $A \otimes B$ конвертируемы и по следствию 1.3.9 матрица $A \otimes B$ конвертируема.

Перейдем к доказательству прямого утверждения. Предположим противное. Так как $\mathrm{per}\,(A) > 0$ и $\mathrm{per}\,(B) > 0$, то в каждой из матриц существует ненулевая обобщенная диагональ. Предположим, что в каждой из матриц A и

B существует не менее двух обобщенных диагоналей без нулевых элементов и матрица $A \otimes B$ конвертируема. Пусть в матрице A выбранные обобщенные диагонали пересекаются по $(n-l)$ элементам. Так как $(n-1)$ элемент однозначно определяет всю обобщенную диагональ, то $l \geq 2$.

Перестановка строк и столбцов матрицы A сохраняет конвертируемость, а значит с помощью этих преобразований ее можно привести к виду:

1. На главной диагонали расположены ненулевые элементы.
2. Элементы $a_{i,i+1} = 1$ для $i = 1, \ldots, l-1$ и $a_{l,1} = 1$.

Полученную матрицу обозначим A'.

Матрица $A' \otimes B$ конвертируема тогда и только тогда, когда конвертируема матрица $B \otimes A'$. Пусть в матрице B две обобщенные диагонали без нулевых элементов пересекаются по $(n-k)$, где $k \geq 2$, элементам. Перестановкой строк и столбцов матрицу B можно привести к матрице B', которая удовлетворяет требованиям

1. На главной диагонали расположены ненулевые элементы.
2. Элементы $b_{i,i+1} = 1$ для $i = 1, \ldots, k-1$ и $a_{k,1} = 1$.

При этом матрица $B' \otimes A'$ конвертируема тогда и только тогда, когда конвертируема матрица $B \otimes A'$.

В матрицах A' и B' все элементы, не входящие в выбранные обобщенные диагонали, заменим нулевыми. Полученные матрицы обозначим A'' и B'' соответственно. Очевидно, что при этом выполнено неравенство:

$$B' \otimes A' \geq B'' \otimes A''. \tag{1.10}$$

Неравенство (1.10) означает, что существует матрица $X \in M_{mn}(0,1)$ такая, что $B'' \otimes A'' = (B' \otimes A') \circ X$. Так как по сделанному предположению матрица $B' \otimes A'$ конвертируема, то согласно следствию 1.3.7 матрица $B'' \otimes A''$ конвертируема.

Выберем в $B'' \otimes A''$ подматрицу C, которая находится на пересечении строк и столбцов с номерами $u + vn$, где $1 \leq u \leq l$ и $0 \leq v \leq (k-1)$. По построению $B'' \otimes A''$ для подматрицы C имеем

$$C = (U_{kk} + I_k) \otimes (U_{ll} + I_l).$$

По лемме 1.4.16 матрица C неконвертируема. Подматрица D, дополняющая C, является главным минором в матрице $B'' \otimes A''$. Так как матрица $B'' \otimes A''$ неотрицательная и элементы ее главной диагонали равны единицам, то per $(D) > 0$. По лемме 1.3.18 матрица $B'' \otimes A''$ неконвертируема. Это противоречит конвертируемости матрицы $A \otimes B$.

Таким образом, одна из матриц содержит единственную обобщенную диагональ. Пусть это верно для матрицы A. Тогда матрица $A \otimes B$ перестановочно эквивалентна блочной верхнетреугольной матрице, где на диагонали стоят блоки B. Следовательно, $A \otimes B$ конвертируема тогда и только тогда, когда конвертируем каждый из блоков B, а значит конвертируема матрица B. Теорема доказана. □

Следствие 1.4.18. Теорема 1.4.17 верна для матриц из $M_n(\mathbb{R}_+)$.

Следствие 1.4.19. Кронекерово произведение матриц $A, B \in M_n(\mathbb{R}_+)$, перманент которых отличен от нуля, конвертируемо тогда и только тогда, когда одна из матриц перестановочно эквивалентна верхнетреугольной, а вторая матрица конвертируема.

Следствие 1.4.20. Пусть $A \in M_n(\mathbb{R}_+)$ — неконвертируемая матрица. Тогда для любой неотрицательной матрицы B выполнено одно из двух утверждений:

1. $\mathrm{per}\,(B) > 0$, тогда матрица $A \otimes B$ неконвертируема.
2. $\mathrm{per}\,(B) = 0$, тогда $\mathrm{per}\,(A \otimes B) = 0$.

Глава 2

Конвертируемые и неконвертируемые (0,1)-матрицы

2.1 Основные определения

Обозначение 2.1.1. Пусть $A \in M_n(0,1)$. Через $\nu(A)$ обозначим число ненулевых элементов матрицы A

Определение 2.1.2. (см. [4]) Максимальное число единиц при котором (0,1)-матрица с положительным перманентом может быть конвертируемой называется верхней границей конвертируемости и обозначается Ω_n. Минимальное число единиц при котором (0,1)-матрица может быть неконвертируемой называется нижней границей конвертации и обозначается ω_n.

Замечание 2.1.3. Теорема 1.2.6 устанавливает точное значение $\Omega_n = \frac{n^2+3n-2}{2}$. Точное значение для нижней границы конвертации может быть получено как следствие теоремы 1.4.11, а также установлено в следующей теореме.

Теорема 2.1.4 (Гутерман, Долинар, Кузьма, [4])**.** Пусть $n \geq 2$, $A \in M_n(0,1)$ и $\nu(A) < \omega_n = n + 6$. Тогда матрица A конвертируема.

Имеет место следующая теорема о существовании конвертируемых и неконвертируемых (0,1)-матриц с числом единиц $r \in [\omega_n, \Omega_n]$.

Теорема 2.1.5 (Гутерман, Долинар, Кузьма, [4]). Для любого $n > 26$ и для любого $r \in [\omega_n, \Omega_n]$ существует знаково неконвертируемая матрица $A \in M_n(0,1)$ с положительным перманентом и числом единиц $\nu(A) = r$.

В [4] была сформулирована следующая задача

Проблема 2.1.6 (Гутерман, Долинар, Кузьма, [4], 2010). Для любого ли целого $r \in [\omega_n, \Omega_n]$, где $3 < n < 26$, существует знаково неконвертируемая матрица $A \in M_n(0,1)$, для которой $\nu(A) = r$?

Конвертацию (0,1)-матриц можно рассматривать и для подмножеств множества (0,1) матриц. В частности, в случае симметрических матриц интересен не только вопрос, когда матрица конвертируема, но и когда конвертация реализуется с помощью симметричной матрицы $X \in M_n(\pm 1)$.

Обозначение 2.1.7. Через $SM_n(X)$ будем обозначать множество симметричных матриц с элементами из X.

Определение 2.1.8. Матрица $A \in SM_n(0,1)$ называется симметрично конвертируемой, если существует матрица $X \in SM_n(\pm 1)$ такая, что $\mathrm{per}\ (A) = \det\ (A \circ X)$. Матрица $A \in SM_n(0,1)$ называется слабо симметрично конвертируемой, если существует симметричная матрица $X \in SM_n(\pm 1)$ такая, что $\mathrm{per}\ (A) = \pm \det\ (A \circ X)$.

Пример 2.1.9. Симметричные матрицы порядка 2 являются слабо симметрично конвертируемыми, конвертация реализуется следующим отображением:

$$\phi \begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix} = \begin{pmatrix} -a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix},$$

но не являются симметрично конвертируемыми.

Известно следующее обобщение теоремы 1.2.6 на симметричные матрицы.

Теорема 2.1.10 (Долинар, Гутерман, Кузьма, [5], теорема 1.4)**.** Пусть $n \geq 3$ и предположим $A \in SM_n$ является симметричной $(0,1)$-матрицей, для которой per $(A) > 0$. Если $\nu(A) = \Omega_n = \frac{n^2+3n-2}{2}$, то A является конвертируемой матрицей тогда и только тогда, когда $A = PT_nP^t$ для некоторой матрицы-перестановки P. Более того, если $n \not\equiv 2 \pmod 4$, то матрица A является симметрично конвертируемой. Если $n \equiv 2 \pmod 4$, тогда A является только симметрично слабо конвертируемой. Здесь через T_n обозначается матрица вида

$$t_{ij} = \begin{cases} 0, \text{ если } i+j \leq n-1 \\ 1, \text{ если } i+j > n-1 \end{cases}$$

перестановочно эквивалентная матрице Гибсона (1.3) и называемая симметричной матрицей Гибсона.

Теорема 2.1.11 (Долинар, Гутерман, Кузьма, [5], теорема 4.4)**.** Пусть $n \geq 3$ и $A \in SM_n(0,1)$ — симметричная $(0,1)$ матрица, у которой $\nu(A) < n+6 = \omega_n$. Тогда матрица A является слабо симметрично конвертируемой.

Понятия симметричной и слабой симметричной конвертации накладывают более сильные ограничения на матрицу.

Лемма 2.1.12. Имеют место следующие утверждения.

1. Если симметричная матрица $A \in SM_n(0,1)$ слабо симметрично конвертируемая (симметрично конвертируемая), то она конвертируемая.

2. Если симметричная матрица $A \in SM_n(0,1)$ неконвертируемая в обычном смысле, то она не является симметрично и слабо симметрично неконвертируемой.

Доказательство. **1**. Если существует симметричная матрица $X \in M_n(\pm 1)$ такая, что $\det\ (X \circ A) = \mathrm{per}\ A$, то матрица A конвертируемая. Если существует только симметричная матрица $Y \in M_n(\pm 1)$ такая, что $\det\ (Y \circ A) = -\mathrm{per}\ A$, то положим матрицу X равной Y, первая строка которой умножена на -1. Получаем $\det\ (X \circ A) = \mathrm{per}\ A$. Таким образом, A конвертируемая.

2. Предположим противное. Пусть матрица симметрично или слабо симметрично конвертируемая. Тогда по пункту 1 матрица должна быть конвертируемой, что противоречит условию. Лемма доказана. □

Проблему 2.1.6 можно переформулировать для симметричных матриц.

Проблема 2.1.13. Верно ли, что для любого целого числа $r \in [\omega_n, \Omega_n]$, где $3 < n < 26$, существует слабо симметрично неконвертируемая матрица $A \in SM_n(0, 1)$, для которой $\nu(A) = r$?

Замечание 2.1.14. В силу определения из слабой симметричной неконвертируемости следует симметричная неконвертируемость.

В силу леммы 2.1.12 достаточно построить симметричные неконвертируемые матрицы с заданным числом ненулевых элементов для решения проблем 2.1.6 и 2.1.13.

Определение 2.1.15. Типом матрицы $A \in M_n(0, 1)$ будем называть пару $(n, \nu(A))$, состоящую из порядка матрицы и числа ненулевых элементов.

2.2 Построение симметричных неконвертируемых (0,1) матриц

В этой части мы полностью разрешим проблему 2.1.13, построив симметричные неконвертируемые матрицы всех возможных типов (n, r), где $r \in [\omega_n, \Omega_n]$.

Таким образом, будет разрешена проблема 2.1.6.

Лемма 2.2.1. Матрицы

$$A_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix},$$

$$A_3 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}, A_4 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

неконвертируемые. При этом $\nu(A_1) = 10, \nu(A_2) = 11, \nu(A_3) = 12, \nu(A_4) = 13.$

Доказательство. Матрица $A_1 = I_1 \oplus J_3$ неконвертируема по лемме 1.3.18.

Неконвертируемость матрицы A_2 следует из более общего утверждения, которое будет доказано ниже (пример 2.3.21).

Для матрицы A_3 имеем $A_3 \circ A_1 = A_1$, по следствию 1.3.7 матрица A_3 неконвертируема.

Для матрицы A_4 имеет место равенство: $\nu(A_4) = \Omega_4$. По теореме 2 эта матрица может быть конвертируемой только если существуют матрицы перестановок P_1, P_2 такие, что $P_1 A_4 P_2$ — матрица Гибсона. Заметим, что в любом столбце и любой строке матрицы A_4 не более одного нулевого элемента. При перестановке строк и столбцов в них не может меняться количество нулевых элементов. В матрице Гибсона G_4 существует столбец с двумя нулевыми элементами. Таким образом, требуемых P_1 и P_2 не существует, и A_4 — неконвертируемая матрица. □

Лемма 2.2.2. Для $n \geq 5$ существует симметричная неконвертируемая матрица A с $\nu(A) = r$ для любого целого $r \in [\omega_n, \Omega_n]$.

Доказательство. Рассмотрим матрицы вида $B = I_{(n-3)} \oplus J_3$ и $C = D \oplus I_{(n-5)} \oplus J_3$, где $D = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. Имеем $\nu(B) = (n+6)$ и $\nu(C) = (n+7)$, матрицы B, C симметричные и неконвертируемые по лемме 1.3.18. Выберем $r \in [\omega_n, \Omega_n]$. Рассмотрим два случая.

1. Если $(r-n)$ четное, то положим $A = B + U$, где $B \circ U = 0$, U симметричная матрица с $(r-n-6)$ единицами. Это возможно сделать, так как $(r-n-6)$ четное число и единичные элементы в U можно выбирать парами, симметричными относительно главной диагонали. Так как $A \circ B = B$, то по следствию 1.3.7 матрица A неконвертируема.

2. Если $(r-n)$ нечетное, то положим $A = C + U$, где $C \circ U = 0$, U симметричная матрица с $(r-n-7)$ единицами. Это возможно сделать, так как $(r-n-7)$ четное и единичные элементы в U можно выбирать парами, симметричными относительно главной диагонали. Так как $A \circ C = C$, то, по следствию 1.3.7, матрица A неконвертируема.

Лемма доказана. □

Таким образом, на основе доказанных лемм 2.2.1 и 2.2.2 можем сформулировать две следующие теоремы, разрешающие сформулированные проблемы 2.1.6 и 2.1.13.

Теорема 2.2.3. Для любого $n \geq 3$ и для любого $r \in [\omega_n, \Omega_n]$ существует неконвертируемая (0,1)-матрица типа (n, r).

Теорема 2.2.4. Для любого $n \geq 3$ и для любого $r \in [\omega_n, \Omega_n]$ существует слабо симметрично неконвертируемая симметричная (0,1)-матрица типа (n, r).

Теорема 2.1.10 позволяет строить примеры симметричных (слабо-)симметрично конвертируемых матриц.

Пример 2.2.5. Рассмотрим матрицу $T_n \in SM_n(0,1)$. Пусть надо построить симметричную слабо симметрично конвертируемую матрицу A с $\nu(A) = r \in [\omega_n, \Omega_n]$ и per $(A) > 0$. Пусть $N = \Omega_n - \nu(A)$. Заменим N любых единиц, кроме лежащих на побочной диагонали, в матрице T_n на нулевые. Получим симметричную матрицу $A \in SM_n(0,1)$ с $\nu(A) = r$ и per $(A) > 0$, так как на побочной диагонали лежат ненулевые элементы. Матрица A конвертируема с помощью той же матрицы $X \in SM_n(\pm 1)$, что и T_n. Построили требуемую матрицу A.

2.3 Нижняя граница конвертации для неразложимых и вполне неразложимых матриц

2.3.1 Понятие неразложимой и вполне неразложимой матриц

Существует несколько эквивалентных определений неразложимой матрицы. Терминология приведена согласно [8] и [2].

Определение 2.3.1. Квадратная матрица $A \in M_n$ называется разложимой, если при некотором разбиении всех индексов $1, \ldots, n$ на две дополнительные непустые системы (без общих индексов) $j_1, \ldots, j_\mu$ и $k_1, \ldots, k_\nu$ $(\mu + \nu = n)$

$$a_{j_\alpha k_\beta} = 0; (\alpha = 1, \ldots, \mu; \beta = 1, \ldots, \nu)$$

В противном случае матрица называется неразложимой.

Определение 2.3.2. Перестановкой рядов в квадратной матрице A называется одновременная одинаковая перестановка строк и столбцов.

Определение 2.3.3. Квадратная матрица $A \in M_n$ называется разложимой, если перестановкой рядов она может быть приведена к виду:

$$A = \begin{pmatrix} B & 0 \\ C & D \end{pmatrix}, \tag{2.1}$$

где B, D — квадратные матрицы. В противном случае матрица A называется неразложимой.

Определение 2.3.4. Неотрицательная матрица $A \in M_n$ называется неразложимой, если для степеней матрицы $A, A^t = (a_{ij}^{(t)})$, при любых i и j существует такое натуральное число $t = t(i,j)$, что $a_{ij}^{(t)} > 0$.

Замечание 2.3.5. В ориентированном графе G допускаются петли и кратные ребра.

Определение 2.3.6. Матрица $A \in M_n(0,1)$ называется матрицей инцидентности ориентированного графа G порядка n, если $a_{ij} = 1$ тогда и только тогда, когда в графе G существует ориентированное ребро $(v_i, v_j) \in E(G)$.

Определение 2.3.7. Ориентированный граф G называется сильно связным, если существует ориентированный путь из любой вершины графа в любую другую вершину.

Определение 2.3.8. Матрица $A \in M_n(0,1)$ называется неразложимой, если она является матрицей смежности сильно связного ориентированного графа.

Понятие разложимости обобщается до понятия частичной разложимости матрицы следующим образом (согласно [8]):

Определение 2.3.9. Квадратную матрицу A порядка n, перестановочно эквивалентную матрице вида

$$\begin{pmatrix} A_1 & * \\ 0 & A_2 \end{pmatrix},$$

где A_1, A_2 — непустые квадратные матрицы, а также нулевую матрицу при $n = 1$, назовем частично разложимой. Если A не является частично разложимой, то она называется вполне неразложимой.

Пользуясь определениями разложимости и частичной разложимости, получаем следующую лемму.

Лемма 2.3.10. Имеют место следующие утверждения.

1. Если матрица A разложимая, то она является частично разложимой.
2. Если матрица A вполне неразложимая, то она является неразложимой матрицей.

Пример 2.3.11. Матрица

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

является неразложимой, но при этом будет частично разложимой, достаточно переставить первый и второй столбец и использовать определение

2.3.2 Операция свертки перманента матрицы и ее свойства

В этой части мы опишем операцию свертки матрицы, с помощью которой для некоторых матриц можно перейти к рассмотрению матрицы меньшего порядка при изучении конвертируемости. Аналогичная конструкция строится в [26] в терминах теории графов.

Определение 2.3.12. Пусть в первой строке неотрицательной матрицы только два ненулевых элемента a_{11}, a_{12}. Сверткой матрицы A по первой строке назовем неотрицательную матрицу $\mathfrak{S}(A)$ следующего вида:

$$\mathfrak{S}(A) = \begin{pmatrix} a_{11}a_{22} + a_{12}a_{21} & a_{23} & \dots & a_{2n} \\ a_{11}a_{32} + a_{12}a_{31} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots \\ a_{11}a_{n2} + a_{12}a_{n1} & a_{n3} & \dots & a_{nn} \end{pmatrix}$$

Из определения свертки матрицы и формулы Лапласа разложения перманента по строке следует следующая лемма.

Лемма 2.3.13. Пусть $A \in M_n(\mathbb{R}_+)$ и существует свертка матрицы A по первой строке, равная $\mathfrak{S}(A)$. Тогда имеет место равенство $\mathrm{per}\ (\mathfrak{S}(A)) = \mathrm{per}\ (A)$.

Лемма 2.3.14. Пусть $A \in M_n(\mathbb{R}_+)$ и существует ее свертка по первой строке, равная матрице $\mathfrak{S}(A)$. Если матрица $\mathfrak{S}(A)$ конвертируема, то конвертируема и матрица A.

Доказательство. Пусть матрица $\mathfrak{S}(A)$ конвертируема с помощью матрицы $X \in M_{n-1}(\pm 1)$. По лемме 2.3.13 имеют место следующие равенства:

$$\mathrm{per}\ (A) = \mathrm{per}\ (\mathfrak{S}(A)) = \det\ (\mathfrak{S}(A) \circ X). \tag{2.2}$$

Используя линейность определителя матрицы, получаем:

$$\det\ (\mathfrak{S}(A) \circ X) = a_{11}\det\ (A(1|1) \circ X) + a_{12}\det\ (A(1|2) \circ X) \tag{2.3}$$

Через A_1 обозначим матрицу, полученную из A заменой всех элементов первой строки и первого столбца, кроме a_{11}, на нули. Аналогично, через A_2 обозначим матрицу, полученную из A заменой всех элементов первой строки и второго столбца, кроме a_{12}, на нули. Через Y обозначим матрицу, полученную из X следующим образом:

$$y_{ij} = \begin{cases} x_{i-1,j-1}, \text{ если } i,j \geq 2 \\ x_{1,j-1}, \text{ если } i = 1, j \geq 2 \\ 1, \text{ если } i = 1, j \neq 2 \\ -1, \text{ если } i = 1, j = 2 \end{cases}$$

С использованием матриц A_1, A_2, Y равенство (2.3) может быть переписано в виде:

$$\det\,(\mathfrak{S}(A) \circ X) = a_{11}\det\,(A_1 \circ Y(1|1)) - a_{12}\det\,(A_2 \circ Y(1|2)) \qquad (2.4)$$

Применим к выражению (2.4) формулу Лапласа разложения определителя по строке и, учитывая выражение (2.2), получаем

$$\mathrm{per}\,(A) = \det\,(\mathfrak{S}(A) \circ X) = \det\,(A \circ Y).$$

Последнее выражение означает, что матрица A конвертируема с помощью матрицы Y, что и требовалось доказать. ☐

Лемма 2.3.15. Пусть $A \in M_n(\mathbb{R}_+)$ и существует ее свертка по первой строке, равная матрице $\mathfrak{S}(A)$. Тогда, если матрица A конвертируема, то конвертируема и матрица $\mathfrak{S}(A)$.

Доказательство. Пусть матрица $X \in M_n(\pm 1)$ конвертирует матрицу A. Без ограничения общности, можно считать, что выполнены следующие условия:

1. В первой строке матрицы A два ненулевых элемента a_{11} и a_{12}.

2. Имеют место равенства: $x_{11} = 1$ и $x_{12} = -1$. Если какое-то из равенств не выполнено, то умножим соответствующий столбец и какую-либо строку, кроме первой, на -1. Новая матрица X' будет конвертировать A, так как $\det(A \circ X) = \det(A \circ X')$.

Докажем, что матрицу X можно выбрать так, что $x_{i1} = x_{i2}$ при $i \geq 2$. Пусть выбранная матрица не удовлетворяет этому условию и существует пара $x_{i1} \neq x_{i2}$ при $i \geq 2$. Если в матрице A один из элементов a_{i1}, a_{i2} равен нулю, то элемент x_{ij} на соответствующем месте можно умножить на -1 и получить равенство $x_{i1} = x_{i2}$.

Предположим теперь, что оба элемента a_{i1}, a_{i2} не равны 0. Возможны два случая:

1. Пусть $\operatorname{per}(A(1i|12)) = 0$. Так как A — неотрицательная матрица, то и подматрица $A(1i|12)$ будет неотрицательной матрицей. Воспользовавшись следствием 1.3.8 получаем равенство:

$$0 = \operatorname{per}(A(1i|12)) = \det(A(1i|12) \circ Y) \quad \text{для любой } \ Y \in M_{n-2}(\pm 1)$$

Это означает, что слагаемое $a_{11}a_{i2}x_{i2}\det((A \circ X)(1i|12))$ не влияет на значение определителя матрицы $A \circ X$ и элемент x_{i2} может быть выбран произвольно, в частности, его можно умножить на -1. Полученная матрица X' конвертирует A и удовлетворяет равенству $x_{i1} = x_{i2}$.

2. Пусть $\operatorname{per}(A(1i|12)) \neq 0$. Разложим определитель по первой строке. Получится два слагаемых с ненулевыми коэффициентами. Разложим определитель соответствующих подматриц по первому столбцу. Получаем равенство:

$$\begin{aligned} \det(X \circ A) = a_{11} \sum_{k=2}^{n} a_{k2}x_{k2}\det((X \circ A)(1k|12)) + \\ + a_{12} \sum_{k=2}^{n} a_{k1}x_{k1}\det((X \circ A)(1k|12)). \end{aligned} \tag{2.5}$$

Аналогичное разложение верно и для перманента матрицы A.

$$\text{per}\ (A) = a_{11}\sum_{k=2}^{n} a_{k2}\text{per}\ (A(1k|12)) + a_{12}\sum_{k=2}^{n} a_{k1}\text{per}\ (A(1k|12)).$$

По следствию 1.3.8 имеем $\text{per}\ (A(1k|12)) \geq |\det\ ((A\circ X)(1k|12))|$ для любого $k \geq 2$. Это означает, что для равенства

$$\text{per}\ (A) = \det\ (A\circ X) \tag{2.6}$$

в выражении (2.5) все слагаемые должны быть положительными. Но так как $x_{i1} = -x_{i2}$, то слагаемые

$$a_{11}a_{i2}x_{i2}\det\ ((A\circ X)(1i|12)) \text{ и } a_{12}a_{i1}x_{i1}\det\ ((A\circ X)(1i|12))$$

имеют разные знаки. Таким образом, выражение (2.6) неверно и матрица A неконвертируема. Это противоречит условиям леммы.

Полученное противоречие доказывает, что матрицу X можно выбрать так, что $x_{i1} = x_{i2}$ при $i \geq 2$.

Раскладывая определитель матрицы $A\circ X$ по первой строке получаем:

$$\det\ (A\circ X) = a_{11}\det\ ((A\circ X)(1|1)) + a_{12}\det\ ((A\circ X)(1|2))$$

Так как для матрицы X имеет место равенство $x_{i1} = x_{i2}$ при $i \geq 2$, то $X(1|1) = X(1|2)$. Подставляя это в последнее равенство и пользуясь леммой 2.3.13 получаем цепочку равенств:

$$\text{per}\ (\mathfrak{S}(A)) = \text{per}\ (A) = \det\ (A\circ X) = \det\ (\mathfrak{S}(A)\circ X(1|1)).$$

Полученное равенство означает, что матрица $\mathfrak{S}(A)$ конвертируема с помощью построенной матрицы $X(1|1)$, что и требовалось доказать. □

Понятие свертки очевидно можно обобщить на случай, когда в неотрицательной матрице A существует строка (столбец) с двумя ненулевыми элементами.

Определение 2.3.16. Пусть в матрица A существует строка с не более чем двумя ненулевыми элементами a_{ij}, a_{ik}, $j < k$. Пусть A' получена из A перестановкой i-той строки на первое место и j-го и k-того столбца на места 1 и 2 соответственно. Матрица A' допускает свертку по первой строке, равную матрице $\mathfrak{S}(A')$. Сверткой матрицы A по i-той строке называется матрица, полученная из $\mathfrak{S}(A')$ перестановкой 1-го столбца на j-тое место.

Замечание 2.3.17. Пусть в матрице A существует столбец i с не более чем двумя ненулевыми элементами. Сверткой матрицы A по i-тому столбцу называется матрица $(\mathfrak{S}(A^t))^t$, где свертка матрицы A^t осуществляется по i-той строке.

Из определения свертки получаем следующую лемму:

Лемма 2.3.18. Пусть в i-той строке матрицы A не более двух ненулевых элементов a_{ij}, a_{ik} и матрица A' получена из A перестановкой i-той строки на первое место и j-го и k-го столбцов на места 1 и 2. Тогда матрицы $\mathfrak{S}(A)$ и $\mathfrak{S}(A')$ перестановочно эквивалентны.

Таким образом, на основании лемм 2.3.14, 2.3.15 и 2.3.18 получаем следующую теорему.

Теорема 2.3.19. Пусть неотрицательная матрица A допускает свертку по строке или столбцу. Тогда матрица A конвертируема в том и только в том случае, когда конвертируема ее свертка $\mathfrak{S}(A)$.

Следствие 2.3.20. Пусть в (0,1)-матрице A существует строка (столбец) с не более чем 2 ненулевыми элементами. Тогда A конвертируема в том и только в том случае, когда конвертируема (0,1)-матрица $\phi(\mathfrak{S}(A))$.

Приведем пример использования теоремы 2.3.19.

Пример 2.3.21. Матрица

$$A = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

неконвертируема. Действительно, матрица A допускает свертку по первой строке и $\mathfrak{S}(A) = J_3$. Так как матрица J_3 неконвертируема, то по теореме 2.3.19 матрица A неконвертируема.

2.3.3 Нижняя граница конвертации

Обозначение 2.3.22. Пусть $A \in M_n(0,1)$. Через $\tau(A)$ обозначим вектор-столбец строчных сумм матрицы A, и через $\tau_i(A)$ — i-тую компоненту этого вектора.

Лемма 2.3.23. Пусть матрица $A \in M_n(0,1)$ допускает свертку по последней строке и $B = \phi(\mathfrak{S}(A))$. Тогда $\tau_i(B) \leq \tau_i(A)$, где $1 \leq i \leq (n-1)$.

Доказательство. Каждая строка матрицы B отличается от соответствующей строки матрицы A тем, что два ее элемента заменены на их линейную комбинацию. Таким образом, число ненулевых элементов в каждой из строк не возросло. Так как строчная сумма элементов (0,1)-матрицы равна числу ненулевых элементов в соответствующей строке, то имеет место неравенство $\tau_i(B) \leq \tau_i(A)$, где $1 \leq i \leq (n-1)$. $\square$

Лемма 2.3.24. Пусть $A \in M_n(0,1)$ и $\tau(A)$ — ее вектор строчных сумм такой, что $\tau_i(A) \leq 2$ при $i \geq 3$. Тогда матрица A конвертируема.

Доказательство. Докажем по индукции. При $n = 2$ все матрицы конвертируемы, а значит база индукции выполнена.

Пусть доказано для всех размеров матриц меньших n. Так как $n \geq 3$, то в последней строке матрицы не более чем 2 ненулевых элемента и можно рассмотреть матрицу $B = \phi(\mathfrak{S}(A))$. По лемме 2.3.23 матрица B порядка $(n-1)$ удовлетворяет условиям настоящей леммы, а значит по предположению индукции матрица B конвертируема. По следствию 2.3.20 конвертируема матрица A, что и требовалось доказать. $\square$

Следствие 2.3.25. Пусть в неотрицательной матрице A не более двух строк с более чем 2 ненулевыми элементами. Тогда матрица A конвертируема.

Теорема 2.3.26. Пусть $A \in M_n(0,1)$ и A — вполне неразложимая матрица. Если $\nu(A) < 2n+3$, то матрица A конвертируема.

Доказательство. Так как матрица A вполне неразложима, то в каждой ее строке не менее 2 ненулевых элементов. Далее, воспользуемся принципом Дирихле. Существует не более 2 строк с тремя и более ненулевыми элементами. По следствию 2.3.25 матрица A будет конвертируема. $\square$

Отметим, что в теореме 2.3.26 доказана точная оценка.

Пример 2.3.27. В разделе 2.4 с точностью до перестановки строк и столбцов описаны все неконвертируемые вполне неразложимые (0,1)-матрицы с $2n+3$ ненулевыми элементами. В частности, показано, что для любого $n \geq 3$ существуют неконвертируемые вполне неразложимые (0,1)-матрицы с $2n+3$ ненулевыми элементами.

Теорема 2.3.26 не обобщается на неразложимые матрицы. Имеет место следующий пример.

Пример 2.3.28. Построим матрицу A по следующему принципу:

1. элементы $a_{i,i+1} = 1$, где $i = 1, \ldots, n-1$;

2. элемент $a_{n,1} = 1$;

3. подматрица, образованная пересечением первых трех строк и второго, третьего и четвертого столбцов, состоит из единиц.

4. остальные элементы матрицы равны нулям.

Очевидно, что при $n \geq 4$ в построенной матрице $n+6$ единичных элементов. Действительно, пункты 1 и 2 дают n ненулевых элементов. По пункту 3 имеем подматрицу с 9 ненулевыми элементами, из которых 3 уже были посчитаны как стоящие над главной диагональю. Данная матрица является матрицей смежности сильно связного графа, что следует из пунктов 1 и 2, а значит является неразложимой. Положим $\alpha = \{4, \dots, n\}$ и $\beta = \{1, 5, \dots, n\}$. Подматрица $A[\alpha|\beta]$ с точностью до перестановки последней строки на первое место совпадает с матрицей I_{n-3}, следовательно per $(A[\alpha|\beta]) > 0$. Подматрица $A(\alpha|\beta) = J_3$ — неконвертируемая. По лемме 1.3.18 матрица A неконвертируема.

Замечание 2.3.29. Последний пример показывает, что для конвертируемости неразложимой матрицы верна только оценка в $\omega_n = (n+6)$ элементов, общая для всех $(0,1)$ матриц.

2.4 Описание неконвертируемых вполне неразложимых (0,1)-матриц с числом единиц на нижней границе конвертации

Лемма 2.4.1. Операция свертки вполне неразложимой (0,1)-матрицы дает вполне неразложимую матрицу.

Доказательство. В силу леммы 2.3.18 можно считать, что дана матрица $A \in M_n(0,1)$ такая, что $a_{11} = a_{12} = 1$ и $a_{1i} = 0$ для $i > 2$. Пусть $B = \mathfrak{S}(A)$.

Докажем утверждение от противного. Предположим, что матрица B частично разложима. Тогда в матрице B существует подматрица C размера $k \times (n-k-1)$, состоящая из нулевых элементов. Возможны два случая.

1. Подматрица C не пересекается с первым столбцом матрицы B. Тогда в A подматрица C не будет пересекаться с 1 и 2 столбцами и первой строкой. Расширим подматрицу C в исходной матрице A путем добавления элементов первой строки. Получим нулевую подматрицу C' порядка $(k+1) \times (n-k-1)$. По определению это означает частичную разложимость матрицы A, что невозможно.

2. Подматрица C пересекается с первым столбцом матрицы B. По построению матрицы B каждому нулевому элементу подматрицы C, лежащему в первом столбце B, соответствует два нулевых элемента матрицы A, которые лежат в соответствующей строке и первом и втором столбцах. Таким образом, подматрицу C можно расширить до нулевой подматрицы C' в матрице A порядка $k \times (n-k)$. По определению это означает частичную разложимость матрицы A, что невозможно.

Полученные противоречия доказывают настоящую лемму. □

Лемма 2.4.2. Пусть $A \in M_n(0,1)$, $n > 3$, вполне неразложимая неконвертируемая матрица с $2n+3$ элементами. Тогда возможно выполнение операции свертки. Более того, имеет место равенство $\nu(A) = \nu(\phi(\mathfrak{S}(A))) + 2$.

Доказательство. В каждой строке матрицы содержится не менее 2 единиц, строк в матрице больше трех. По принципу Дирихле существует строка строго с двумя единичными элементами. Таким образом, возможно выполнение операции свертки.

При операции свертки из матрицы вычеркивается строка с двумя ненулевыми элементами. Имеет место неравенство:

$$\nu(\phi(\mathfrak{S}(A))) \leq 2n + 1 \tag{2.7}$$

По теореме 2.3.19 и следствию 1.3.7 матрица $\phi(\mathfrak{S}(A))$ неконвертируема, и по лемме 2.4.1 вполне неразложима. По теореме 2.3.26 имеет место неравенство:

$$\nu(\phi(\mathfrak{S}(A))) \geq 2(n-1) + 3 = 2n + 1 \tag{2.8}$$

Объединяя неравенства (2.7) и (2.8), получаем второе утверждение леммы. □

Следствие 2.4.3. Пусть $A \in M_n(0,1)$ вполне неразложимая неконвертируемая матрица с $\nu(A) = (2n+3)$. Тогда имеют место утверждения:

1. Если свертка осуществляется по i-той строке и $a_{ik} = a_{il} = 1$, то ни для какого $m \neq i$ не возможно равенство $a_{mk} = a_{ml} = 1$.

2. Если свертка осуществляется по j-тому столбцу и $a_{kj} = a_{lj} = 1$, то ни для какого $m \neq j$ не возможно равенство $a_{km} = a_{lm} = 1$.

3. Свертка по i-той строке(столбцу) $\mathfrak{S}(A)$ является $(0,1)$-матрицей.

Доказательство. Действительно, если выполнено равенство $a_{mk} = a_{ml} = 1$ при каком-то $m \neq i$, то при операции свертки эти единичные элементы будут заменены на один элемент, а значит количество ненулевых элементов в матрице уменьшится минимум на три, что противоречит результату леммы 2.4.2.

Для доказательства второй половины утверждения достаточно рассмотреть матрицу A^t и применить уже полученный результат к строкам матрицы.

Последнее утверждение напрямую следует из первых двух, так как не существует пары $(a_{mk}, a_{ml}) = (1, 1)$, где $m \neq i$. $\square$

Следствие 2.4.4. Любую вполне неразложимую неконвертируемую матрицу $A \in M_n(0, 1)$ с $2n+3$ единичными элементами можно привести к матрице J_3 последовательным применением операции свертки.

Доказательство. По лемме 2.4.2 операция свертки при $n > 3$ возможна. По лемме 2.4.1 результатом операции свертки будет вполне неразложимая матрица. По следствию 2.4.3 результатом операции свертки будет (0,1)-матрица. Таким образом, имеет место равенство $\nu(A) = \nu(\mathfrak{S}(A)) + 2$, а матрица $\mathfrak{S}(A)$ является вполне неразложимой неконвертируемой матрицей порядка $(n-1)$ с $2(n-1)+3$ ненулевыми элементами. Таким образом, к матрице $\mathfrak{S}(A)$ можно повторить операцию свертки. Продолжим, пока $n > 3$. В случае если $n = 3$, то мы получим вполне неразложимую неконвертируемую (0,1)-матрицу с 9 элементами, которая совпадает с J_3. $\square$

Определение 2.4.5. Расширением (0,1)-матрицы A по i-тому столбцу будем называть множество матриц $\mathfrak{R}(A)$ такое, что для каждой $B \in \mathfrak{R}(A)$ имеем $B \in M_{n+1}(0, 1)$, $b_{1,i} = b_{1,i+1} = 1$ и $\mathfrak{S}(B) = A$.

Замечание 2.4.6. Непосредственно из определения операций свертки и расширения следует, что если $B \in \mathfrak{R}(A)$ и $b_{1i} = b_{1,i+1} = 1$, то в каждой паре $(b_{1i}, b_{1,i+1})$ не менее одного нулевого элемента.

Лемма 2.4.7. Пусть Y — множество вполне неразложимых неконвертируемых (0,1)-матриц порядка n с $(2n+3)$ ненулевыми элементами. Тогда любая вполне неразложимая неконвертируемая матрица A порядка $(n+1)$ с $2(n+1)+3$ элементами перестановочно эквивалентна одной из матриц из множества $\cup_{B \in Y} \mathfrak{R}(B)$, где в объединении берутся расширения по всем столбцам матриц B.

Доказательство. По лемме 2.3.18 строки и столбцы матрицы можно переставить таким образом, что свертка осуществляется по первой строке и в первой строке два соседних элемента равны единицам. При этом результирующая матрица будет перестановочна эквивалентна той матрице, которая получается в результате свертки до перестановки строк. Таким образом, без ограничения общности, можно считать, что $a_{1i} = a_{1,i+1} = 1$, а остальные элементы первой строки A равны нулям. По пункту 1 следствия 2.4.3 для каждой пары $(a_{m,i}, a_{m,i+1})$, где $i \geq 2$, известно, что как минимум один элемент равен нулю. По лемме 2.4.1 получаем, что $\mathfrak{S}(A) \in Y$, а значит согласно определению расширения имеем $A \in \mathfrak{R}(\mathfrak{S}(A))$. Лемма доказана. □

Обозначение 2.4.8. Через R_n обозначим матрицу порядка n, определенную по правилу:

$$r_{ij} = \begin{cases} 1, \text{ если } i + j = n \text{ или } i + j = n + 1 \\ 0, \text{ иначе.} \end{cases} \tag{2.9}$$

Матрица R_k является основным блоком при описании неконвертируемых $(0, 1)$-матриц с $2n + 3$ единичными элементами. Поэтому начнем доказательство со следующей леммы.

Лемма 2.4.9. Пусть $R_n \in M_n(0, 1)$ и $B \in \mathfrak{R}(R_n)$, где расширение взято не по последнему столбцу и в каждом столбце B не более двух ненулевых элементов. Тогда существуют матрицы перестановки P, Q такие, что $R_{n+1} = PBQ$. Более того, матрицы P и Q оставляют неподвижными последнюю строку и последний столбец матрицы B.

Доказательство. Пусть расширение выполнено по столбцу с номером $k < n$ на столбцы с номерами k и $k+1$. При этом столбцы с номером меньше k остаются на месте, а столбцы с номером больше k сдвигаются на один вправо. Новая строка в матрице B ставится на первое место.

По построению в k-том столбце R_n есть два ненулевых элемента $r_{n-k,k}, r_{n-k+1,k}$. Элемент $r_{n-k,k}$ перейдет в элементы $(b_{n-k+1,k}, b_{n-k+1,k+1})$, один из которых равен нулю. Аналогично $r_{n-k+1,k}$ перейдет в элементы $(b_{n-k+2,k}, b_{n-k+2,k+1})$, один из которых равен нулю.

Заметим, что равенство:

$$b_{n-k+1,k} = b_{n-k+2,k} = 0$$

невозможно, так как тогда элементы $b_{1,k+1}, b_{n-k+1,k+1}, b_{n-k+2,k+1}$ отличны от 0, что противоречит условию леммы. Аналогично невозможно равенство

$$b_{n-k+1,k+1} = b_{n-k+2,k+1} = 0$$

Остается рассмотреть два случая:

1. Элемент $r_{n-k,k}$ перешел в элемент $b_{n-k+1,k+1}$, а элемент $r_{n-k+1,k}$ перешел в элемент $b_{n-k+2,k}$. В качестве матрицы Q в этом случае выберем тождественную перестановку.

2. Элемент $r_{n-k,k}$ перешел в элемент $b_{n-k+1,k}$, а элемент $r_{n-k+1,k}$ перешел в элемент $b_{n-k+2,k+1}$. Так как $b_{1,k} = b_{1,k+1} = 1$, то матрицы в первом и втором случаях отличаются перестановкой столбцов с номерами k и $k+1$. Определим Q как матрицу перестановки указанных столбцов.

Таким образом, в матрице BQ в первой строке два ненулевых элемента на k-ом и $(k+1)$-ом местах, а матрица $BQ(1|)$ имеет вид:

$$BQ(1|) = \begin{pmatrix} O'_{n-k,k+1} & R_{n-k} \\ R_k & O_{k,n-k+1} \end{pmatrix},$$

где матрица $O'_{n-k,k+1}$ отличается от нулевой наличием единичного элемента в правом нижнем углу. При действии построенной перестановки Q последний столбец остается на своем месте.

Для получения матрицы R_{n+1} из BQ поставим первую строку этой матрицы между $(n{-}k{+}1)$-ой и $(n{-}k{+}2)$-ой строками. Этой операции соответствует циклический сдвиг первых $(n-k+1)$ строк с $\sigma = (n-k+1, n-k, \dots, 2, 1) \in S_{n+1}$. В качестве P выберем матрицу, соответствующую перестановке σ. При таком выборе P последняя строка матрицы B сохранит свое положение. Лемма доказана. □

Определение 2.4.10. Будем говорить, что выполнена операция расширения (0,1)-матрицы A с выбором, если выбрана одна из матриц из множества $\mathfrak{R}(A)$.

Лемма 2.4.11. Пусть дана матрица размера 3 на 1 (вектор-столбец размера 3), заполненная единицами. К этой матрице k раз применили операцию расширения с выбором, и получили матрицу B размера $(k+3) \times (k+1)$. Пусть после каждого шага в каждом столбце полученной матрицы не менее 2 ненулевых элементов. Тогда существуют целые неотрицательные числа k_1, k_2 и k_3, где $k_1 + k_2 + k_3 = k$, и матрицы перестановок P, Q строк и столбцов матрицы B такие, что матрица PBQ имеет следующий вид:

$$T = \begin{pmatrix} V_{k_1} & O_{k_1,k_3} & O_{k_1,k_2} & R_{k_1} \\ V_{k_2} & O_{k_2,k_3} & R_{k_2} & O_{k_2,k_1} \\ V_{k_3} & R_{k_3} & O_{k_3,k_2} & O_{k_3,k_1} \\ W_0 & W_3 & W_2 & W_1 \end{pmatrix} = \begin{pmatrix} \overline{C_k} \\ \overline{W_k} \end{pmatrix} \tag{2.10}$$

где:

1. V_{k_i} — вектор столбец из k_i элементов с единственным единичным элементом, стоящим на последнем месте, если $k_i > 0$, и пустой вектор, если $k_i = 0$.

2. W_0 — вектор столбец из трех элементов.

3. В первом столбце матрицы (2.10) три ненулевых элемента.

4. Каждая из подматриц W_i, где $i = 1, 2, 3$, имеет размеры $3 \times k_i$ и при $k_i > 0$ имеет единственный ненулевой элемент, который находится в i-той строке в последнем столбце.

5. В каждой строке подматрицы $\overline{W_k} = \begin{pmatrix} W_0 & W_3 & W_2 & W_1 \end{pmatrix}$ содержится единственный единичный элемент.

Замечание 2.4.12. В выражение (2.10) матрица разбита на блоки $\overline{W_k}$ и $\overline{C_k}$, где k означает число проделанных операций расширения с выбором, $\overline{W_k}$ включает в себя три последние строки полученной матрицы, а $\overline{C_k}$ включает все строки, кроме 3 последних.

Доказательство. Докажем индукцией по k — количеству произведенных расширений. Очевидно, что при $k = 0$ условия леммы выполнены.

Пусть после k расширений существуют матрицы перестановки P, Q такие, что PBQ удовлетворяет всем условиям леммы. Без ограничения общности можно считать, что $(k+1)$-ое расширение применяется к матрице A вида (2.10). По определению операции расширения если при расширении расщепляется m-тый столбец, то новые столбцы имеют номера m и $m+1$, а новая строка ставится на первое место в $B = \mathfrak{R}(A)$. При этом порядок других строк и столбцов сохраняется.

Столбцы в матрице B делятся на три различных класса:

1. Столбец с двумя единичными элементами, не являющийся крайним правым для одного из блоков R_{k_i}.

2. Столбец с двумя единичными элементами, являющийся крайним правым для одного из блоков R_{k_i}.

3. Столбец с тремя единичными элементами. Данный столбец является первым в матрице B.

Построим матрицы перестановок P, Q для каждого из трех описанных случаев.

Случай 1. Пусть при расширении расщепляется один из столбцов, пересекающийся с блоком R_{k_1}, кроме последнего столбца этого блока. Рассмотрим подматрицу

$$C = B[1, \ldots, k_1 + 1 | 2 + k_2 + k_3, \ldots, k + 2].$$

Подматрица C является расширением матрицы R_{k_1} по первой строке и не последнему столбцу. По лемме 2.4.9 существуют такие перестановки строк и столбцов, что подматрица примет вид R_{k_1+1}. Применим эти перестановки строк и столбцов к подматрице C, оставляя неподвижными остальные строки и столбцы матрицы B. Полученную матрицу обозначим через D.

Проверим, что при этом сохраняется общий вид матрицы. Очевидно, что $V_{k_2}, V_{k_3}, W_2, W_3, W_0$ и нулевые блоки сохранили свой вид. По лемме 2.4.9 $(k_1 + 1)$-ая строка матрицы B останется на своем месте, а значит вектор V_{k_1+1} в этой матрице будет иметь единственный единичный элемент на последнем месте. Таким образом, выполнены условия 1 и 2. При перестановке столбцов последний столбец остается на месте, а значит выполнено условие 3. В подматрице W_1 добавится один нулевой столбец, после чего столбцы этой подматрицы, кроме последнего, переставлены, а значит выполнено условие 4. Так как три последние строки не переставляются, то условие 5 выполнено.

Случай 2. Пусть при расширении расщепляется последний столбец подматрицы R_{k_1} и всей матрицы A. Это столбец с номером $k + 1$. В $(k + 1)$-ом столбце матрицы A ровно два единичных элемента. Так как расширение выполняется без расщепления ненулевых элементов, то эти элементы должны перейти в элементы, лежащие в различных столбцах матрицы B. Иначе в B существует столбец с единственным ненулевым элементом, что противоречит условию.

Если элемент $a_{1,k+1}$ перешел в элемент $b_{2,k+1}$ матрицы B, то элемент $a_{k+1,k+1}$ перешел в элемент $b_{k+2,k+2}$. Тогда матрица B имеет вид (2.10), где блок R_{k_1} заменен на блок R_{k_1+1}. Если элемент $a_{1,k+1}$ перейшел в $b_{2,k+2}$, то переставим два последних столбца матрицы B. Получим матрицу вида (2.10). Действительно, в обоих случаях правый верхний блок будет иметь вид R_{k_1+1}, нулевые блоки сохранят свое положение, в блоке W_1 единичный элемент будет в последнем столбце и последние три строки сохранят свой порядок, а значит выполнены условия 2-5. В векторе V_{k_1} добавиться нулевой элемент вначале, что означает выполнение условия 1.

Случаи 1' и 2'. Для рассмотрения блоков R_{k_2} и R_{k_3} переставим их на место блока R_{k_1}. При этом общий вид матрицы (2.10) сохранится. Воспользуемся уже доказанным утверждением для блока R_{k_1}. Затем переставим блоки в прежнем порядке.

Случай 3. Пусть при расширении расщепляется первый столбец. Так как в этом столбце три единичных элемента, то в силу условий леммы два из них должны остаться в одном столбце, а один перейти в другой. Без ограничения общности, можно считать, что два из трех элементов первого столбца матрицы A перешли в первый столбец матрицы B, а один из них перешел во второй столбец. В частности, это означает, что для матрицы B выполнено условие 3.

Предположим, что единичный элемент из W_0 перешел во второй столбец. В силу пунктов 3, 4 и 5 это означает, что одно из чисел k_i было равно нулю. Без ограничения общности, можно считать, что для матрицы A имеем $k_1 = 0$. В этом случае переставим второй столбец на последнее место. Единичный элемент в правом верхнем углу будет подматрицей R_1, единичный элемент в левом верхнем углу будет вектором столбцом из одного элемента $V_{k_1} = V_1$, векторы столбцы V_{k_2} и V_{k_3} остаются без изменения, а значит выполнено 1. W_1 будет матрицей размера 3×1, которая содержит единственный единичный элемент, W_2, W_3 остаются без изменения, а значит выполнено 4. Последнии три строки не переставлялись и содержат те же единичные элементы, а значит выполнено 5 и 2. Таким образом, полученная матрица удовлетворяет условиям леммы.

Предположим, что единичный элемент не из W_0 перешел во второй столбец. Без ограничения общности, можно считать, что это элемент из V_1 и $k_1 > 0$. Переставим первую строку матрицы B на $(k_1 + 1)$-ое место, а второй столбец на $(k_2 + k_3 + 2)$-ое место. Полученную матрицу обозначим через D.

Остается проверить, что D удовлетворяет всем требованиям леммы. В правом верхнем углу матрицы D находится блок R_{k_1+1} образованный блоком R_{k_1} с приписанным к нему слева столбцом порядка (k_1+1) с единичными элементами на двух последних местах, и дополненный нулями до матрицы порядка $(k_1 + 1)$. Нулевые блоки сохранили свое положение, блоки R_{k_2} и R_{k_3} не меняются при описанных преобразованиях. В левом верхнем углу D расположен вектор столбец порядка $(k_1 + 1)$ с единственным единичным элементом на последнем месте, который обозначим за V_{k_1+1}, а вектора V_{k_2}, V_{k_3} не изменялись, значит выполнено 1. В последние три строки добавился один столбец, заполненный нулями, который был переставлен на $(k_2 + k_3 + 2)$-ое место и включен первым в блок W_1 для D, другие столбцы не переставлялись, а значит выполнены условия 4 и 5. Условие 2 выполняется автоматически, а значит полученная матрица D удовлетворяет всем условиям леммы.

Таким образом, требования леммы выполнены после каждого шага расширения, в частности, после фиксированного k-того шага. Лемма доказана.
$\square$

Основываясь на результате леммы 2.4.11 получаем следующее утверждение:

Теорема 2.4.13. Пусть $n \geq 3$. Для любой вполне неразложимой неконвертируемой матрицы $A \in M_n(0,1)$ с $\nu(A) = 2n + 3$ существуют неотрицательные целые числа m_1, m_2, m_3 такие, что $m_1 + m_2 + m_3 + 3 = n$ и матрица A с точностью до перестановки строк и столбцов имеет вид:

$$\begin{pmatrix} \overline{C_{m_1}} & O_{m_1,m_2+1} & O_{m_1,m_3+1} \\ O_{m_2,m_1+1} & \overline{C_{m_2}} & O_{m_2,m_3+1} \\ O_{m_3,m_1+1} & O_{m_3,m_2+1} & \overline{C_{m_3}} \\ \overline{W_{m_1}} & \overline{W_{m_2}} & \overline{W_{m_3}} \end{pmatrix} \tag{2.11}$$

где $\overline{C_{m_i}}$ и $\overline{W_{m_i}}$ — блоки матрицы T, которая задана формулой (2.10), а $O_{i,j}$ нулевая подматрица порядка $i \times j$.

Доказательство. Обозначим за Y множество вполне неразложимых неконвертируемых матриц порядка n с $(2n+3)$ единичными элементами. За X обозначим множество вполне неразложимых неконвертируемых матриц порядка $(n-1)$ с $(2(n-1)+3)$ единичными элементами. Как было доказано в лемме 2.4.7, все матрицы множества Y могут быть получены из матриц множества X с помощью операций расширения. Кроме того, на каждом шаге расширения в каждом столбце полученной матрицы не менее двух ненулевых элементов, иначе она частично разложима.

Выберем матрицу $A \in X$, имеющую вид (2.11). Без ограничения общности, можно считать, что выполняется операция расширения с расщеплением одного из (k_1+1) первых столбцов, и выбрана одна из результирующих матриц $B \in \mathfrak{R}(A)$, содержащая не менее двух единиц в каждом столбце. Рассмотрим подматрицу

$$D = B[1, \ldots, m_1 + 1, n - 1, n, n + 1|1, \ldots, k + 1] \in \mathfrak{R}(\begin{pmatrix} C_{m_1} \\ W_{m_1} \end{pmatrix}).$$

К последнему расширению применим результат леммы 2.4.11, а значит существуют перестановки строк и столбцов P', Q', пересечение которых образует D, что будет выполнено равенство $P'DQ' = \begin{pmatrix} C_{m_1+1} \\ W_{m_1+1} \end{pmatrix}$, где матрицы C_{m_1+1} и W_{m_1+1} удовлетворяют требованиям теоремы. Столбцы и строки, не входящие в подматрицу D в матрице B сохранят свое положение. Доопределим P', Q' до матриц P, Q соответствующим образом. Получаем, что матрица PBQ имеет вид (2.11), что и требовалось доказать.

Если расширение выполнено с расщеплением столбца, который пересекается с C_{m_2}, то переставим первую строку на $(m_1 + 1)$-ое место и в качестве A рассмотрим матрицу, лежащую на пересечение столбцов с $(m_1 + 1)$-го до (m_1+m_2)-го и строк, соответствующих C_{m_2}, W_{m_2} и строки с номером (m_1+1). Аналогично для C_{m_3}. Таким образом, теорема полностью доказана. □

Глава 3

Матрицы над конечными полями

3.1 Введение

В этой главе рассматривается аналог знаковой конвертации перманента в определитель для матриц над конечным полем. Данное направление исследований обусловлено следующей теоремой:

Теорема 3.1.1 (Вазирани, Янакакис, [44], теорема 5.1). Пусть A — целочисленная матрица. Тогда для любого $k > 1$, не являющегося степенью двойки, проверка $\text{per}\,(A) = \det\,(A) (\text{mod } k)$ является NP-сложной задачей по любому модулю k даже для $(0, 1)$-матриц.

В случае простого k последнюю теорему можно рассматривать как переход в поле из k элементов. Конечная характеристика поля обуславливает несколько существенных изменений при исследовании понятия конвертации. Это приводит к тому, что не выполняются аналоги теорем, запрещающих конвертацию для неотрицательных матриц. С другой стороны, так как конвертация неотрицательных матриц эквивалентна знаковой невырожденности, то любая матрица над конечным полем с тем же расположением ненулевых элементов, что и конвертируемая неотрицательная матрица, будет конвертируемой.

Другой подход к построению отображения $T : M_n \to M_n$ такого, что выполнено равенство

$$\text{per}\,(A) = \det\,(T(A)) \tag{3.1}$$

изучался в работе [17], где предполагалось, что отображение T биективно. Такой подход можно охарактеризовать как биективная конвертация. Была рассмотрена следующая задача.

Проблема 3.1.2. Для каких $n \geq 3$ и для каких конечных полей $\mathbb{F}_q$, характеристика которых больше двух, существует биективное отображение $T : M_n(\mathbb{F}_q) \to M_n(\mathbb{F}_q)$, для которого выполнено равенство (3.1) для любой матрицы $A \in M_n(\mathbb{F}_q)$?

Для этой задачи было получено следующее асимптотическое решение:

Теорема 3.1.3 (Долинар, Гутерман, Кузьма, Орел, [17])**.** Для любого $n \geq 3$ существует такое $Q = Q(n)$, что для любого конечного поля $\mathbb{F}_q$, характеристики которого больше двух и $|\mathbb{F}_q| > Q(n)$ не существует биективного отображения

$$T : M_n(\mathbb{F}_q) \to M_n(\mathbb{F}_q),$$

такого, что выполнено равенство (3.1) для любой матрицы $A \in M_n(\mathbb{F}_q)$.

Кроме знаковой конвертации, в этой части изучается биективный подход. Разрабатывается новая техника вычисления перманента, которая позволяет доказать не асимптотический аналог теоремы 3.1.3.

3.2 Конвертация матриц над конечным полем

Обозначение 3.2.1. Через $\mathbb{F}_q$ будем обозначать конечное поле из q элементов, где $q = p^k$ и p простое число. Если $q = p$, то будем писать $\mathbb{F}_q = \mathbb{F}_p$.

Обозначение 3.2.2. В случае матриц над конечным полем через $\phi(A)$ будем обозначать матрицу, полученную из A заменой всех ненулевых элементов на единицы.

Теорема 3.2.3. Пусть $A \in M_n(\mathbb{F}_q)$ и $B \in M_n(0, 1)$, причем B рассматривается как матрица над полем комплексных чисел. Тогда, если матрица B конвертируема и $\phi(A) \leq B$, то матрица A конвертируема как матрица над полем $\mathbb{F}_q$.

Доказательство. Матрица B конвертируема, значит существует матрица $X \in M_n(\pm 1)$ такая, что $X \circ B$ знаково невырождена. Это означает, что в записи определителя $\det\ (X \circ B)$ все слагаемые, отвечающие ненулевым обобщенным диагоналям матрицы B, входят с плюсом. Так как $\phi(A) \leq B$, то множество перестановок, отвечающих ненулевым обобщенным диагоналям в A, является подмножеством перестановок, отвечающих ненулевым обобщенным диагоналям в B. Таким образом, в $\det\ (X \circ A)$ все слагаемые, отвечающие ненулевым обобщенным диагоналям матрицы, входят с тем же знаком, что и в $\mathrm{per}\ (A)$. Получаем требуемое равенство $\det\ (X \circ A) = \mathrm{per}\ (A)$. $\square$

Следствие 3.2.4. Пусть $A \in M_n(\mathbb{F}_q)$ и число ненулевых элементов в A меньше $(n + 6)$. Тогда матрица A конвертируема.

Замечание 3.2.5. Оценка $(n + 6)$ в следствии 3.2.4 является точной. Ниже будет доказано, что существуют неконвертируемые матрицы над конечным полем с $(n + 6)$ ненулевыми элементами.

Результаты, запрещающие знаковую конвертацию некоторых неотрицательных матриц в случае поля с конечной характеристикой уже верны не всегда.

Пример 3.2.6. Матрица J_3 конвертируема как матрица над $\mathbb{F}_3$. Действительно, непосредственно из определения перманента и определителя матрицы имеем:

$$\mathrm{per}\begin{pmatrix}1 & 1 & 1\\ 1 & 1 & 1\\ 1 & 1 & 1\end{pmatrix} = 0 = \det\begin{pmatrix}1 & 1 & 1\\ 1 & 1 & 1\\ 1 & 1 & 1\end{pmatrix}$$

Замечание 3.2.7. В примере 1.2.7 показано, что в случае характеристики поля равной двум имеет место равенство $\mathrm{per}\,(A) = \det\,(A)$. Таким образом, рассмотрение знаковой конвертации в случае конечного поля имеет смысл только при $\mathrm{char}\,(\mathbb{F}_q) \geq 3$.

3.2.1 Конвертация матриц над полем из 3 элементов

Начнем с рассмотрения простейшего из конечных полей, характеристика которого больше двух. Наша цель доказать конвертируемость всех матриц над $\mathbb{F}_3$. Также будут построены примеры неконвертируемых матриц для любого $n \geq 3$ и конечного поля $\mathbb{F}_q$, где $\mathrm{char}\,\mathbb{F}_q > 2$ и $|\mathbb{F}_q| > 3$.

Лемма 3.2.8. Пусть $A \in M_n(\mathbb{F}_3)$ и $\mathrm{per}\,(A) \neq 0$. Тогда существует такая матрица $X \in M_n(\pm 1)$, что $\det\,(A \circ X) = \mathrm{per}\,(A)$.

Доказательство. Докажем по индукции, что если $\mathrm{per}\,(A) \neq 0$, то существует матрица $X \in M_n(\pm 1)$ такая, что $\det\,(A \circ X) \neq 0$.

Построим матрицу X. Начнем с $X = J_n$. Укажем те элементы, которые необходимо умножить на минус один. Доказательство проведем по индукции.

База при $n = 2$. Пусть

$$A = \begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}.$$

Тогда в качестве матрицы X возьмем

$$X = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

По определению перманента и определителя получаем равенство $\text{per }(A) = \det (X \circ A)$.

Пусть утверждение индукции доказано для матриц, размер которых не более $(n-1)$. Докажем для $A \in M_n(\mathbb{F}_3)$. Положим $X = J_n$. Если $\det (A) \neq 0$, то изменять X не требуется.

Предположим, что $\det (A) = 0$. Разложим определитель A по первой строке:

$$\det (A) = a_{11}\det (A(1|1)) - \ldots + (-1)^{n+1}a_{1n}\det (A(1|n)).$$

Предположим, что существует такой номер j, что $a_{1j}\det (A(1|j)) \neq 0$. Умножим x_{1j} на минус один.

$$\det (A \circ X) = \det (A) - (-1)^{1+j}x_{1j}a_{1j}\det (A(1|j)) =$$

$$= \det (A) \pm 2 = \mp 1.$$

Получили требуемую матрицу X.

Предположим, что не существует номера j такого, что $a_{1j}\det (A(1|j)) \neq 0$. Так как $\text{per }(A) \neq 0$, то в силу формулы Лапласа существует k такое, что $a_{1k}\text{per }(A(1|k)) \neq 0$. Воспользуемся предположением индукции для подматрицы $A(1|k)$. Существует матрица $Y \in M_n(\pm 1)$ такая, что $\det (A(1|k) \circ Y(1|k)) \neq 0$.

Для матрицы $Y \circ A$ в разложении определителя по первой строке существует ненулевое слагаемое. По ранее доказанному, существует матрица $Z \in M_n(\pm 1)$ такая, что $\det (Z \circ (Y \circ A)) \neq 0$. Положим $X = Z \circ Y$. Очевидно, что X искомая матрица.

Доказали, что если per $(A) \neq 0$, то существует матрица X такая, что det $(A \circ X) \neq 0$. Если per $(A) =$ det $(A \circ X)$, то лемма доказана. Если per $(A) = -$det $(A \circ X)$, то умножим элементы первой строки матрицы X на минус один. Построили требуемую матрицу X. Лемма доказана. □

Лемма 3.2.9. Пусть дано $k \geq 2$ ненулевых элементов из $\mathbb{F}_3$. Тогда линейной комбинацией этих элементов с коэффициентами ± 1 можно получить любой элемент из $\mathbb{F}_3$.

Доказательство. Пусть $k = 2$. Так как ненулевые элементы из $\mathbb{F}_3$ — это ± 1, а коэффициенты в линейной комбинации это ± 1, то, без ограничения общности, можно считать, что даны два единичных элемента. С помощью требуемых линейных комбинаций из этих двух единиц можно получить любой элемент $\mathbb{F}_3$:

1. $1 - 1 = 0$
2. $-1 - 1 = -2 = 1$
3. $1 + 1 = 2 = -1$

Пусть $k > 2$. Можно считать, что все k элементов равны единицам. Первые $(k-2)$ элемента возьмем с коэффициентом $+1$. Беря различные линейные комбинации последних двух единиц, можно получить любой элемент поля $\mathbb{F}_3$. Выбрав нужную комбинацию и прибавив ее к уже сложенным $(k-2)$ элементам, можем получить любой элемент поля $\mathbb{F}_3$, что и требовалось доказать. □

Лемма 3.2.10. Пусть $A \in M_n(\mathbb{F}_3)$. Пусть per $(A) = 0$. Тогда существует такая матрица $X \in M_n(\pm 1)$, что det $(A \circ X) = 0$.

Доказательство. Если det $(A) = 0$, то положим $X = J_n$.

При $n = 2$ выберем

$$X = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

Получаем равенство $0 = \mathrm{per}\,(A) = \det\,(A \circ X)$.

Пусть утверждение леммы доказано для матриц, порядкок которых не превосходит $(n-1)$. Докажем для матриц порядка n. Предположим, что det $(A) \neq 0$. Построим матрицу X такую, что столбцы $X \circ A$ линейно зависимы. Положим $X = J_n$ и выясним, какие элементы X надо умножить на -1.

Рассмотрим количество ненулевых элементов в строках матрицы A. Пусть в каждой строке есть как минимум два ненулевых элемента. Это означает, что в сумме $\sum\limits_{j=1}^{n} a_{ij}x_{ij}$ есть как минимум два ненулевых элемента для любого фиксированного $i = 1, \ldots, n$. Применим к каждой из этих сумм лемму 3.2.9. Изменение знаков при слагаемых можно считать изменением знаков при x_{ij}. Для полученной матрицы X выполнены равенства $\sum\limits_{j=1}^{n} a_{ij}x_{ij} = 0$ для любого i. Это означает, что строки матрицы $X \circ A$ линейно зависимы над $\mathbb{F}_3$ с коэффициентами $\lambda_1 = \ldots = \lambda_n = 1$. Построили требуемую X.

Строки из нулевых элементов нет, так как это бы противоречило предположению det $(A) \neq 0$. Остается рассмотреть случай, когда в A существует строка с единственным ненулевым элементом. Переставим строки и столбцы матрицы так, чтобы этот элемент оказался на месте $(1, 1)$. Получим матрицу вида:

$$PAQ = A^{(1)} = \begin{pmatrix} \pm 1 & 0 & \ldots & 0 \\ a_{21}^{(2)} & \ldots & & \\ & \ldots & & \end{pmatrix}.$$

где P, Q — матрицы перестановок. Имеет место равенство:

$$0 = \text{per } (A) = \text{per } (A^{(1)}) = a_{11}^{(1)}\text{per } (A^{(1)}(1|1))$$

Так как $a_{11}^{(1)} \neq 0$, то per $(A^{(1)}(1|1)) = 0$. По предположению индукции для $A^{(1)}(1|1)$ можно указать $Y \in M_n(\pm 1)$ такую, что выполнено равенство:

$$\det\ (A^{(1)} \circ Y) = a_{11}y_{11}\det\ (A^{(1)}(1|1) \circ Y(1|1)) = 0.$$

Так как

$$0 = \det\ (P^{-1}(A^{(1)} \circ Y)Q^{-1}) = \det\ (A \circ (P^{-1}YQ^{-1})),$$

то в качестве искомой матрицы X положим $X = P^{-1}YQ^{-1}$. Лемма доказана. □

Теорема 3.2.11. Пусть $A \in M_n(\mathbb{F}_3)$, тогда существует $X \in M_n(\pm 1)$ такая, что per $(A) = \det\ (A \circ X)$.

Доказательство. Пусть per $(A) = 0$. По лемме 3.2.10 существует матрица $X \in M_n(\pm 1)$ такая, что $\det\ (X \circ A) = 0$.

Пусть per $(A) = 1$. По лемме 3.2.8 существует матрица $X \in M_n(\pm 1)$ такая, что $\det\ (X \circ A) = 1$.

Пусть per $(A) = -1$. Возьмем $Y \in M_n(\pm 1)$ такую, что отличается от J_n умножением всех элементов первой строки на -1. Положим $B = A \circ Y$. Тогда per $(B) = 1$. По лемме 3.2.8 существует матрицы $Z \in M_n(\pm 1)$ такая, что:

$$1 = \det\ (Z \circ B) = \det\ (Z \circ Y \circ A)$$

Полагая $X = Z \circ Y$, завершаем доказательство теоремы. □

Пример 3.2.12. Матрица

$$A = \begin{pmatrix} x+1 & 2 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

неконвертируема для любого поля $\mathbb{F}_q$, характеристика которого равна 3, а число элементов $q > 3$. В этом примере поле $\mathbb{F}_q$ представлено как фактор-кольцо кольца $\mathbb{F}_3[x]$ по соответствующему многочлену. Таким образом, поле $\mathbb{F}_3$ является единственным полем характеристики 3, для которого любая матрица конвертируема.

Доказательство. По определению перманента:

$$\mathrm{per}\begin{pmatrix} x+1 & 2 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = 2x + 8 = 2x + 2$$

Предположим противное, пусть существует матрица $X \in M_3(\pm 1)$, конвертирующая A. Так как коэффициент при x равен

$$\pm\mathrm{det}\,((A \circ X)(1|1)) = \pm\mathrm{det}\,(X(1|1)) \neq 0,$$

то подматрица $X(1|1)$ невырождена. Это означает, что с точностью до умножения строк и столбцов матрицы X на минус один получим равенство

$$X(1|1) = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

Это возможно сделать, так как если в X четное количество строк и столбцов умножить на минус один, то полученная матрица также будет конвертировать A.

Так как $\mathrm{det}\,(X(1|1)) = 2$ и $\mathrm{char}\,(\mathbb{F}_q) = 3$, то для равенства коэффициентов при x необходимо, чтобы $x_{11} = 1$. В зависимости от выбора элементов x_{21} и x_{31} определитель одной из подматриц $X(1|2), X(1|3)$ равен нулю, а второй ± 2. Разложим определитель матрицы $A \circ X$ по первой строке:

$$\mathrm{det}\,(A) = 2(x+1) - 2x_{12}\mathrm{det}\,(X(1|2)) + x_{13}\mathrm{det}\,(X(1|3)). \tag{3.2}$$

Рассмотрим два возможных варианта:

1. Пусть $\det\,(X(1|2)) = 0$. Тогда (3.2) примет вид $\det\,(A) = 2(x+1) \pm 2 \neq 2x+2$.

2. Пусть $\det\,(X(1|3)) = 0$. Тогда (3.2) примет вид $\det\,(A) = 2(x+1) \mp 4 \neq 2x+2$.

Таким образом, доказана неконвертируемость матрицы A. □

Лемма 3.2.13. Пусть $B \in M_3(\pm 1) \subset M_3(\mathbb{F}_q)$, где $\mathrm{char}\,(\mathbb{F}_q) = p > 3$. Тогда $\det\,(B) \neq 2$.

Доказательство. Рассмотрим матрицу $A = J_3$. Матрица B может быть получена из A путем последовательного умножения некоторых элементов на -1.

В матрице A шесть обобщенных диагоналей и каждое из диагональных произведений равно единице. В выражении для $\det\,(A)$ три диагональных произведения взяты с плюсом и три с минусом. Докажем, что четность числа слагаемых в $\det\,(A)$, взятых с минусом, есть инвариант при умножении элементов матрицы на -1.

Умножение элемента матрицы A на -1 влияет на знак двух слагаемых в записи определителя. Имеем следующие три варианта.

1. Два слагаемых поменяют знак с плюса на минус. Количество отрицательных слагаемых увеличится на два и четность сохранится.

2. Два слагаемых поменяют знак с минуса на плюс. Количество отрицательных слагаемых уменьшится на два и четность сохранится.

3. Слагаемые имеют разные знаки. Их знаки поменяются, число отрицательных слагаемых при этом не изменится, так как нулевых слагаемых среди них нет. Следовательно, четность сохранится.

Всего в определителе A три слагаемых с минусом. Таким образом, после каждого умножения элемента матрицы A на -1 одно из 6 слагаемых в $\det(A)$ должно быть с минусом, значит, количество слагаемых с минусом в $\det(A)$ может быть равно 1, 3 или 5. Это соответствует элементам 4, 0 и -4 поля $\mathbb{F}_q$. В силу того, что $\operatorname{char}(\mathbb{F}_q) \geq 5$ ни одно из этих чисел не равно 2, а значит $\det(B) \neq 2$. □

Теорема 3.2.14. Для всякого поля $\mathbb{F}_q$, такого, что $\operatorname{char}(\mathbb{F}_q) \geq 3$ и $|\mathbb{F}_q| \geq 5$, и для любого $n \geq 3$ существует неконвертируемая матрица $A \in M_n(\mathbb{F}_q)$.

Доказательство. Выберем неконвертируемую матрицу B порядка 3. Если $\operatorname{char}(\mathbb{F}_q) = 3$, то положим матрицу B равной матрице, построенной в примере 3.2.12. Если $\operatorname{char}(\mathbb{F}_q) > 3$, то положим

$$B = \begin{pmatrix} -1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

По определению $\operatorname{per}(B) = 2$. По лемме 3.2.13 не существует матрицы $X \in M_n(\pm 1)$ такой, что $\det(B \circ X) = 2$, а значит матрица B неконвертируема.

В качестве искомой матрицы порядка n возьмем матрицу A, построенную в виде прямой суммы $A = I_{n-3} \oplus B$. Неконвертируемость матрицы A следует из неконвертируемости матрицы B. □

Пример 3.2.15. Из теоремы 3.2.11 и доказательства теоремы 3.2.14 следует, что матрица

$$\begin{pmatrix} -1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

может быть, как конвертируемой, так и неконвертируемой, в зависимости от выбора поля.

3.2.2 Построение примеров знаково конвертируемых матриц

Определение 3.2.16. Пусть $A \in M_n(\mathbb{F}_q)$. Существенный элемент a_{ij} матрицы A будем называть существенно не равным нулю в смысле определителя, если выполнено неравенство: $a_{ij}\mathrm{det}\ (A(i|j)) \neq 0$, и существенно не равным нулю в смысле перманента, если $a_{ij}\mathrm{per}\ (A(i|j)) \neq 0$.

Лемма 3.2.17. Пусть $A \in M_n(\mathbb{F}_q)$, где $\mathrm{char}\ (\mathbb{F}_q) = p > 3$ и n не делится на p, имеет вид:

$$A = \begin{pmatrix} 2+\delta_1 & 2 & 2 & \dots & 2 & 3+\delta_0 \\ 1 & 2+\delta_2 & 2 & \dots & 2 & 1 \\ \dots & \dots & \dots & \dots & \dots & \\ 1 & \dots & \dots & 2+\delta_{n-2} & 2 & 1 \\ 1 & \dots & \dots & 1 & 2+\delta_{n-1} & 1 \\ 1 & 1 & \dots & \dots & 1 & 1 \end{pmatrix} \tag{3.3}$$

и выполнены следующие условия:

1. $\delta_i = 1$, где $i \geq 1$, если $(2n - i)$ делится на p и ноль иначе;
2. $\delta_0 = 1$ если $2n + 1$ делится на p и 0 в противном случае.

Тогда $\mathrm{rank}(A) = n$ и сумма элементов любой строки построенной матрицы не равна нулю.

Доказательство. Приведем элементарными преобразованиями матрицу A к ступенчатому виду.

1. Вычтем первый столбец из всех остальных, учитывая, что $\delta_1 = 0$. Получим матрицу вида:

$$\begin{pmatrix} 2+\delta_1 & 0 & 0 & \dots & 0 & 1+\delta_0 \\ 1 & 1+\delta_2 & 1 & \dots & 1 & 0 \\ \dots & \dots & \dots & \dots & \dots & \\ 1 & \dots & \dots & 1+\delta_{n-2} & 0 & 0 \\ 1 & \dots & \dots & 0 & 1+\delta_{n-1} & 0 \\ 1 & 0 & \dots & \dots & 0 & 0 \end{pmatrix}$$

Последняя строка полученной матрицы содержит единственный ненулевой элемент в левом нижнем углу матрицы.

2. Вычтем последнюю строку из всех остальных с требуемыми коэффициентами, чтобы в первом столбце остался единственный ненулевой элемент a_{n1}.

3. Переставим последний и первый столбцы. В результате получим верхнетреугольную матрицу с ненулевыми элементами на диагонали, а значит определитель не равен 0 и $\text{rank}(A) = n$.

Проверим, что сумма элементов в любой строке на равна 0. Сумма элементов первой строки исходной матрицы равна $(2n + 1 + \delta_0)$. По условию δ_0 подобрано так, что $(2n+1+\delta_0) \neq 0$. Сумма элементов k-той строки исходной матрицы, где $k > 1$, равна

$$(k-1) + (n-k) * 2 + 1 + \delta_k = 2n - k + \delta_k.$$

Таким образом, ноль возможен только в тех строках, для которых $(2n - k)$ делится на p, но по условию $\delta_k = 1$ для этих строк, а значит сумма элементов в этих строках $(2n-k+1) \neq 0$. По условию n не делится на p, а значит сумма элементов последней строки не делится на p. □

Лемма 3.2.18. Пусть $A \in M_n(\mathbb{F}_q)$, где $\mathrm{char}\,\mathbb{F}_q = p > 3$ и n делится на p, имеет вид:

$$A = \begin{pmatrix} 2+\delta_1 & 2 & 2 & \dots & 2 & 1 \\ 1 & 2+\delta_2 & 2 & \dots & 2 & 1 \\ \dots & \dots & \dots & \dots & \dots & \\ 1 & \dots & \dots & 2+\delta_{n-2} & 2 & 1 \\ 1 & \dots & \dots & 1 & 2+\delta_{n-1} & 1 \\ 1 & 1 & \dots & \dots & 1 & 2 \end{pmatrix} \tag{3.4}$$

где $\delta_i = 1$ если $(2n-i)$ делится на p и ноль иначе. Тогда $\mathrm{rank}(A) = n$. Также для матрицы A сумма элементов каждой строки не равна нулю.

Доказательство. Приведем матрицу A к ступенчатому виду с помощью элементарных преобразований.

1. Учитывая, что $\delta_1 = 0$, вычтем первый столбец из всех остальных. Получим матрицу вида:

$$\begin{pmatrix} 2+\delta_1 & 0 & 0 & \dots & 0 & -1 \\ 1 & 1+\delta_2 & 1 & \dots & 1 & 0 \\ \dots & \dots & \dots & \dots & \dots & \\ 1 & \dots & \dots & 1+\delta_{n-2} & 1 & 0 \\ 1 & \dots & \dots & 0 & 1+\delta_{n-1} & 0 \\ 1 & 0 & \dots & \dots & 0 & 1 \end{pmatrix}$$

Последний столбец полученной матрицы содержит два ненулевых элемента.

2. Прибавим последнюю строку к первой. Так как $\mathrm{char}\,(\mathbb{F}_q) > 3$, то полученная матрица будет содержать единственный нулевой элемент в первой строке на месте (1,1).

3. Вычитая первую строку из всех остальных с коэффициентом 3^{-1}, оставим единственный ненулевой элемент в первом столбце. В результате этого получили верхнетреугольную матрицу с ненулевыми элементами на главной диагонали, а значит определитель не равен нулю и $\operatorname{rank}(A) = n$.

Проверим, что сумма элементов в любой строке на равна 0. Сумма элементов первой строки исходной матрицы $(2n - 1 + \delta_1) = -1$, так как n делится на p и $\delta_1 = 0$. Сумма элементов k-той строки исходной матрицы, где $n > k > 1$, равна

$$(k - 1) + (n - k) * 2 + 1 + \delta_k = 2n - k + \delta_k.$$

Таким образом, ноль возможен только в тех строках, для которых $(2n - k)$ делится на p, но по условию леммы при таких значениях k имеем $\delta_k = 1$, а значит сумма элементов в этих строках $2n - k + 1 \neq 0$. Для последней строки сумма элементов равна $(n+1) = 1$, так как n делится на p по условию леммы, где p — характеристика поля. $\square$

Лемма 3.2.19. Пусть поле $\mathbb{F}_q$ характеристики $p > 3$. Рассмотрим матрицы (3.3),(3.4). Припишем к матрице (3.3) или (3.4) столбец, равный сумме всех остальных столбцов. Тогда для полученной матрицы $\overline{A} \in M_{n+1,n}(\mathbb{F}_q)$ выполнены следующие условия:

1. Элементы $\overline{A}$ не равны нулю.
2. Любая подматрица порядка n матрицы $\overline{A}$ невырождена и, следовательно, ее ранг равен n.

Доказательство. По определению, матрицы (3.3) и (3.4) не содержат ненулевых элементов, значит достаточно проверить, что последний столбец $\overline{A}$ не содержит нулевых элементов. По леммам 3.2.17 и 3.2.18 сумма элементов каждой строки этих матриц не равна 0, а значит вектор, полученный как сумма векторов столбцов, не будет содержать нулей, и все элементы $\overline{A}$ не равны нулю.

Докажем, что Любая подматрица порядка n матрицы $\overline{A}$ невырождена. Предположим противное. Пусть в матрице $\overline{A}$ существует вырожденная подматрица $\overline{A}(|k), k \leq n+1$. Матрица $\overline{A}$ выбрана так, что подматрица $\overline{A}(|n+1)$ заведомо невырождена. Предположим, что $k \neq (n+1)$. Без ограничения общности, можно считать, что $k = 1$. Для матрицы $\overline{A}(|1)$ вычтем все столбцы из последнего. По построению последнего столбца, получится столбец, равный первому столбцу матрицы $\overline{A}(|n+1)$. Это означает, что получили матрицу, отличающуюся от $\overline{A}(|n+1)$ перестановкой столбцов. Таким образом, матрица $\overline{A}(|1)$ невырождена. Лемма доказана. □

Лемма 3.2.20. Рассмотрим поле $\mathbb{F}_p$, где p — простое число. Пусть даны $(p-1)$ ненулевой элемент $a_1, \dots, a_{p-1}$ поля $\mathbb{F}_p$. Тогда линейной комбинацией вида $\sum\limits_{i=1}^{p-1}(-1)^{\alpha_i}a_i$ можно получить любой элемент поля $\mathbb{F}_p$.

Доказательство. Будем последовательно увеличивать на один количество элементов и оценивать снизу количество различных значений, которые могут принимать всевозможные линейные комбинации этих элементов со знаками ±1. Рассмотрим элемент a_1. Так как $\mathrm{char}\ (\mathbb{F}_q) \neq 2$, то $a_1 \neq -a_1$. Таким образом, для одного элемента получили две различные линейные комбинации заданного вида. Далее будем добавлять по одному элементу, и смотреть сколько линейных комбинаций может быть получено.

Пусть на k-том шаге, $k < (p-1)$, получили K разных элементов поля $\mathbb{F}_p$ как линейные комбинации элементов $a_1, \dots, a_k$ с коэффициентами ±1. Обозначим их $\{A_1, \dots, A_K\}$. Добавим $(k+1)$-ый элемент.

1. Количество полученных различных элементов поля в виде линейных комбинаций не может уменьшиться. Действительно, среди новых линейных комбинаций заданного вида $\sum\limits_{i=1}^{k+1}(-1)^{\alpha_i}a_i$ будут и K комбинаций $\sum\limits_{i=1}^{k}(-1)^{\alpha_i^{A_j}}a_i + a_{k+1} = A_j + a_{k+1}$. То есть, к K различным элементам поля прибавили фиксированную константу, а значит получили K различных элементов поля.

2. Пусть $K < p$. Покажем, что при добавлении a_{k+1} в линейную комбинацию количество полученных различных элементов поля строго увеличивается. Предположим противное: количество полученных элементов не изменилось. Числа из множества $\{A_1 + a_{k+1}, \dots, A_K + a_{k+1}\}$ попарно различны. Они равны тем элементам поля $\mathbb{F}_p$, которые можно получить как комбинацию $a_1, \dots, a_{k+1}$. Это же верно и для $\{A_1 - a_{k+1}, \dots, A_K - a_{k+1}\}$. В силу сделанного предположения, данные множества должны совпадать, а значит верно следующее тождество:

$$\sum_{i=1}^{K}(A_i + a_{k+1}) = \sum_{i=1}^{K}(A_i - a_{k+1})$$

Раскрывая скобки, получаем:

$$Ka_{k+1} = -Ka_{k+1}$$

Перенося всё в одну сторону, получаем

$$2Ka_{k+1} = 0$$

Что неверно, так как $\mathrm{char}\,(\mathbb{F}_p) = p$ — простое число и $K < p$.

3. Если $K = p$, то по пункту 1 число различных элементов поля $\mathbb{F}_p$, полученных как линейные комбинации не уменьшилось, а в силу числа элементов в поле не могло и увеличиться. Таким образом, осталось равным p после добавления a_{k+1}.

Завершим доказательство леммы. Элемент a_1 дал две различные комбинации. После этого к нему были добавлены еще $(p-2)$ ненулевых элемента, при этом добавление нового элемента увеличивало количество полученных различных элементов из поля как минимум на один, пока не были получены все элементы $\mathbb{F}_p$. Таким образом, после добавления получим не менее

$2 + (p-2) = p$ различных комбинаций, то есть любой элемент поля. Что и требовалось доказать. □

Следствие 3.2.21. Рассмотрим поле $\mathbb{F}_p$, где p — простое число. Пусть даны $k > (p-1)$ ненулевой элемент $a_1, \ldots, a_{p-1}$ поля $\mathbb{F}_p$. Тогда линейной комбинацией вида $\sum\limits_{i=1}^{p-1}(-1)^{\alpha_i}a_i$ можно получить любой элемент поля $\mathbb{F}_p$.

Доказательство. Дано $k > p-1$ ненулевых элементов. Разделим их на две группы: $a_1, \ldots, a_{p-1}$ и $a_p, \ldots, a_k$. Согласно лемме 3.2.20 комбинациями элементов $a_1, \ldots, a_{p-1}$ можно получить любой элемент поля. Добавим к каждой полученной комбинации сумму элементов $a_p, \ldots, a_k$. Результатом всех комбинаций по-прежнему будет любой элемент $\mathbb{F}_p$. □

Следствие 3.2.22. Пусть даны $a_1, \ldots, a_k$ — не равные нулю элементы поля $\mathbb{F}_p$, где $\mathrm{char}\,(\mathbb{F}_p) = p > 2$ и $k < p$. Тогда линейными комбинациями $\sum\limits_{i=1}^{k}(-1)^{\delta_i}a_i$, где $\delta \in \{0,1\}$, можно получить минимум k различных ненулевых элементов поля $\mathbb{F}_p$, но не менее 2.

Доказательство. В доказательстве леммы 3.2.20 при добавление l-того элемента число различных чисел, полученных в виде $\sum\limits_{i=1}^{l}(-1)^{\delta_i}a_i$ было не менее $l+1$. Один из элементов может быть равен 0. Таким образом, при добавлении k-того числа в линейную комбинацию получим не менее k чисел отличных от нуля.

При $k = 1$ будет две линейные комбинации: a_1 и $-a_1$, при этом $a_1 \neq -a_1$, так как характеристика поля отлична от двух. Таким образом, количество различных ненулевых элементов не меньше двух. □

Лемма 3.2.23. Пусть матрица $A \in M_n(\mathbb{F}_q)$ не содержит ненулевых элементов. Тогда существует такая матрица $X \in M_n(\pm 1)$, что $\mathrm{per}\ (A \circ X) \neq 0$.

Доказательство. Есил per $(A) \neq 0$, то положим $X = J_3$.

Предположим per $(A) = 0$. Докажем по индукции. Для $n = 2$ матрица имеет вид:

$$B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix},$$

где $b_i \neq 0$. Получаем: per $(B) = b_1 b_4 + b_2 b_3$. Если предположить, что per $(B) = 0$, тогда для матрицы B' вида

$$B' = \begin{pmatrix} b_1 & b_2 \\ -b_3 & b_4 \end{pmatrix}$$

перманент не равен нулю. Действительно, если для матриц B и B' перманент равен 0, то, складывая их, получаем:

$$\text{per }(B) + \text{per }(B') = b_1 b_4 + b_2 b_3 + b_1 b_4 - b_2 b_3 = 2 b_1 b_4 \neq 0,$$

так как характеристика поля отлична от 2 и $b_1, b_4 \neq 0$.

Разложим матрицу A по первой строке:

$$\text{per }(A) = \sum_{i=1}^{n} a_{1i} \text{per }(A(1|i)) \tag{3.5}$$

Существует две возможности:

1. В разложении (3.5) существует ненулевой элемент. Тогда по следствию 3.2.22 между элементами суммы (3.5) можно расставить знаки так, что она будет отлична от 0. Предположим, что знаки изменены у слагаемых $a_{1i_1}\text{per }(A(1|i_1)), \ldots, a_{1i_k}\text{per }(A(1|i_k))$. Тогда в качестве матрицы X возьмем J_n, в которой элементы первой строки $x_{1i_1}, \ldots, x_{1i_k}$ умножили на минус один. Получаем неравенство:

$$\text{per }(A \circ X) = \sum_{i=1}^{n} x_{1i} a_{1i} \text{per }(A(1|i) \circ X(1|i)) \neq 0$$

2. Предположим, что в разложении (3.5) все слагаемые равны нулю. Воспользуемся предположением индукции. Для матрицы $A(1|1)$ можно подобрать матрицу $Y \in M_n(\pm 1)$ такую, что per $(A(1|1) \circ Y(1|1)) \neq 0$. Тогда в разложении

$$\text{per } (A \circ Y) = \sum_{i=1}^{n} y_{1i} a_{1i} \text{per } (A(1|i) \circ Y(1|i))$$

первое слагаемое заведомо будет не равно нулю.

Применим к матрице $A \circ Y$ уже доказанное в пункте 1 утверждение. Построенную матрицу обозначим Z. Тогда верно неравенство per $(A \circ Y \circ Z) \neq 0$. Положим $X = Y \circ Z$. Лемма доказана. □

Теорема 3.2.24. Пусть $\mathbb{F}_q$ — поле характеристики $p \geq 3$. Тогда для любого $n \geq (p-1)$ существует конвертируемая матрица с ненулевым перманентом, которая не содержит нулевых элементов.

Доказательство. Заметим, что так как $\mathbb{F}_p \subset \mathbb{F}_q$, где char $(\mathbb{F}_q) = p$, то теорему достаточно доказать для поля $\mathbb{F}_p$ для любого простого $p \geq 3$.

В случае $p = 3$ результат настоящей теоремы следует из теоремы 3.2.11, так как конвертируемой будет любая матрица без нулевых элементов.

Если $(n-1)$ не делится на p, то выберем матрицу A равной матрице, построенной в лемме 3.2.17. Если $(n-1)$ делится на p, то выберем матрицу A равной матрице, построенной в лемме 3.2.18. По лемме 3.2.19 к матрице A можно приписать столбец из ненулевых элементов и получить матрицу $\overline{A} \in M_{n-1,1}(\mathbb{F}_p)$ без нулевых элементов такую, что любая подматрица в ней порядка $(n-1)$ будет невырожденной. К матрице $\overline{A}$ припишем первую строку из единичных элементов. Полученную матрицу обозначим через C.

Согласно лемме 3.2.23 существует матрица $Y \in M_n(\pm 1)$ такая, что per $(C \circ Y) = P \neq 0$.

Теперь разложим определитель матрицы C по первой строке:

$$\det(C)=\sum_{i=1}^{n}(-1)^{i+1}c_{1i}\det(C(1|i))=\sum_{i=1}^{n}\det(\overline{A}(1|i)) \tag{3.6}$$

Из построения матрицы C следует, что сумма (3.6) состоит из n ненулевых слагаемых. Так как $n\geq(p-1)$, то по лемме 3.2.21 слагаемые в (3.6) можно умножить на ±1 так, чтобы получить любой элемент поля $\mathbb{F}_p$, в частности P. Возьмем теперь матрицу $Z\in M_n(\pm1)$, где минус единицы находятся только в первой строке на i-том месте, если в сумме (3.6) i-тое слагаемое умножено на минус один. Получаем равенство:

$$\mathrm{per}\,(C\circ Y)=P=\det(C\circ Z)$$

Положим $X=Y\circ Z$ и $D=C\circ Y$. Получаем равенство $\mathrm{per}\,(D)=\det(D\circ X)$. Таким образом, для любого $n\geq(p-1)$ построили конвертируемую матрицу с ненулевым перманентом, которая не содержит нулей. Лемма доказана. □

Замечание 3.2.25. Теорема 3.2.24 демонстрирует для матриц над конечным полем невозможность введения запрета на конвертацию с помощью оценок снизу на количество ненулевых элементов.

3.2.3 Достаточные условия знаковой конвертации матрицы над конечным полем

Следующая лемма обобщает лемму 3.2.23.

Лемма 3.2.26. Пусть в матрице $A\in M_n(\mathbb{F}_p)$, $p>2$, существует ненулевая обобщенная диагональ. Тогда существует такая матрица $X\in M_n(\pm1)$, что $\mathrm{per}\,(A\circ X)\neq0$.

Доказательство. Без ограничения общности можно считать, что главная диагональ матрицы A заполнена ненулевыми элементами. Этого можно добиться перестановкой столбцов исходной матрицы.

Докажем по индукции. Пусть $n = 2$. Если per $(A) \neq 0$, то положим $X = J_2$ — матрица порядка 2, заполненная единичными элементами. Очевидно, что лемма выполнена. Предположим, что

$$\text{per } (A) = a_{11}a_{22} + a_{12}a_{21} = 0.$$

Так как на главной диагонали стоят ненулевые элементы, то

$$a_{11}a_{22} \neq 0 \quad \text{и} \quad a_{11}a_{22} = -a_{12}a_{21} \neq 0.$$

Положим

$$X = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

Так как char $(\mathbb{F}_p) = p > 2$, то

$$\text{per } (A \circ X) = a_{11}a_{22} - a_{12}a_{21} = 2a_{11}a_{22} \neq 0.$$

Пусть $n > 2$ и утверждение доказано для всех матриц, порядок которых меньше n. По предположению индукции существует такая матрица $X \in M_n(\pm 1)$, что per $((A \circ X)(1|1)) \neq 0$. Применим формулу Лапласа к перманенту матрицы $A \circ X$:

$$\text{per } (A \circ X) = \sum_{i=1}^{n} a_{1i}x_{1i}\text{per } ((A \circ X)(1|i)). \tag{3.7}$$

Первое слагаемое в (3.7) не равно нулю. Если per $(A \circ X) \neq 0$, то X — искомая матрица. Если per $(A \circ X) = 0$, то умножим в X элемент x_{11} на -1. Тогда

$$\text{per } (A \circ X) = -2a_{11}x_{11}\text{per } (A(1|1) \circ X(1|1)) \neq 0.$$

Построили требуемую матрицу X. Лемма доказана. □

Следствие 3.2.27. Пусть в матрице $A \in M_n(\mathbb{F}_p)$, $p > 2$, существует ненулевая обобщенная диагональ. Тогда существует такая матрица $X \in M_n(\pm 1)$, что det $(A \circ X) \neq 0$.

Доказательство. Доказательство дословно повторяет доказательство леммы 3.2.26 с заменой перманента на определитель. □

Следствие 3.2.28. Пусть $A \in M_n(\mathbb{F}_p)$ и $\mathrm{per}\,(A) \neq 0$, $p > 2$. Тогда существует матрица $X \in M_n(\pm 1)$ такая, что $\det\,(A \circ X) \neq 0$.

Доказательство. Так как $\mathrm{per}\,(A) \neq 0$, то в матрице существует обобщенная диагональ, состоящая из ненулевых элементов. Утверждение следует из следствия 3.2.27. □

Теорема 3.2.29. Пусть матрица $A \in M_n(\mathbb{F}_p)$, где $p > 2$ и $n \geq 2p - 6$, удовлетворяет следующим условиям:

1. Один из столбцов не содержит нулевых элементов.

2. В одной из строк не менее

$$M = (p-3)\log(n-1)(p-1) + 2$$

ненулевых элементов.

3. Матрица A вполне неразложима.

Тогда матрица A конвертируема.

Доказательство. Без ограничения общности, можно считать, что первый столбец матрицы A не содержит нулевых элементов, а первая строка A содержит m ненулевых элементов, причем $m \geq M$. Этого можно добиться перестановкой столбца без нулевых элементов на первое место и строки с максимальным количеством ненулевых элементов на первое место. При этом свойство конвертируемости матрицы сохраняется.

Так как матрица A вполне неразложима, то для любой нулевой подматрицы размера $s \times t$ имеем $(t + s) \leq (n - 1)$. Следовательно, для любой ненулевой подматрицы $l \times k$ в $A(1|1)$ имеем $(l + k) \leq (n - 1)$. Построим по матрице $A(1|1)$ (0,1)-матрицу B того же порядка, элементы которой равны 1 тогда и только тогда, когда элемент матрицы $A(1|1)$, расположенный на том же месте, не равен нулю. В матрице B для любой $l \times k$ подматрицы имеет место неравенство $(l+k) \leq (n-1)$. Применим к B, как матрицы над вещественными числами, теорему Фробениуса-Кенега. Получаем, что в B существует обобщенная диагональ без нулевых элементов. Из построения матрицы B следует, что в $A(1|1)$ существует ненулевая обобщенная диагональ. По следствию 3.2.28 можно выбрать такую матрицу $Y \in M_n(\pm 1)$, что $\det\left((A \circ Y)(1|1)\right) \neq 0$. Поэтому можно считать, что для матрицы A выполнено условие $\det\left(A(1|1)\right) \neq 0$.

Рассмотрим строки матрицы $A(|1)$ как элементы векторного пространства $V^{n-1}(\mathbb{F}_p)$. Обозначим их через $a_1, \ldots, a_n$. Так как $\det\left(A(1|1)\right) \neq 0$, то вектора $a_2, \ldots, a_n$ линейно независимы. Пусть

$$N = \{a_1 \circ v, \text{ где } v \in V^{n-1}(\pm 1)\}.$$

Так как в векторе a_1 имеется $(m-1)$ ненулевая компонента, а характеристика поля равна $p > 2$, то в N существует в точности 2^{m-1} различных векторов.

Так как $\det\left(A(1|1)\right) \neq 0$, то существует обратная к $A(1|1)$ матрица. Обозначим ее через $B = (A(1|1))^{-1}$. Через e_k, $k = 1, \ldots, n-1$, обозначим вектор длинны $(n-1)$ такой, что k-тая координата равна 1, а остальные 0. Из определения B следует, что $a_i B = e_{i-1}$ для $i = 2, \ldots, n$. Пусть $N' = NB$. Очевидно, что N' содержит 2^{m-1} различных векторов.

Докажем, что в N существует элемент, который выражается минимум через $(p-2)$ вектора a_i, $i = 2, \ldots, n$. Так как вектор a_i перешел в вектор e_{k-1} при умножении на матрицу B, то требуемое утверждение равносильно тому, что в N' существует вектор с $(p-2)$ ненулевыми координатами.

Предположим противное. Посчитаем, сколько может быть в множестве N'

векторов менее чем с $(p-2)$ ненулевым координатами, обозначим их количество через D. Они включают в себя вектора с одной ненулевой компонентой, всего $(n-1)(p-1)$ штук, вектора с двумя ненулевыми компонентами, всего $C^2_{n-1}(p-1)^2$ штук и так далее, вплоть до векторов с $(p-3)$ различными ненулевыми компонентами, всего $C^{p-3}_{n-1}(p-1)^{p-3}$. Складывая, получаем следующую оценку:

$$D = \sum_{i=1}^{p-3} C^i_{n-1}(p-1)^i \tag{3.8}$$

В силу сделанного предположения имеет место неравенство $D \geq |N'|$.

Оценим величину D сверху. Заметим, что при $i < (p-3) \leq \frac{n}{2}$ имеет место неравенство:

$$\frac{C^i_{n-1}(p-1)^i}{C^{i+1}_{n-1}(p-1)^{i+1}} = \frac{i+1}{(n-i-1)(p-1)} < \frac{1}{p-1} \tag{3.9}$$

Выражение (3.9) означает, что каждое следующее слагаемое в сумме (3.8) как минимум в $(p-1)$ раз больше предыдущего, а значит всю сумму можно оценить сверху удвоенным последним слагаемым:

$$D < 2C^{p-3}_{n-1}(p-1)^{p-3}. \tag{3.10}$$

Логарифмируя неравенство $D \geq |N'|$ по основанию 2, получаем:

$$\begin{gathered} M - 1 \leq m - 1 \leq \log D = \\ \log 2 + (p-3)\log(p-1) + \sum_{k=n-p+3}^{n-1} \log k - \sum_{j=2}^{p-3} \log j \end{gathered} \tag{3.11}$$

Уберем из $\log D$ отрицательные слагаемые, а положительные приравняем максимальному. Используя условия леммы, получим:

$$\log D < \log 2 + (p-3)\log(p-1) + (p-3)\log(n-1) =$$
$$= (p-3)\log(n-1)(p-1) + 1 = M - 1 \leq m - 1 \qquad (3.12)$$

Неравенства (3.11) и (3.12) противоречат друг другу, а значит существует элемент в N' не менее чем с $(p-2)$ ненулевыми координатами.

В силу построения множества N' это означает, что в N существует вектор, который выражается минимум через $(p-2)$ вектора из $a_2, \ldots, a_n$.

Выберем вектор, выражающийся не менее чем через $(p-2)$ вектора. Обозначим его через $b = a_1 \circ v$. Выберем матрицу X такую, что первая строка без первого элемента совпадают с v, а остальные элементы единичные. Далее рассмотрим матрицу $C = A \circ X$. Обозначим через c_1 первую вектор-строку в матрице $C(|1)$. Для матрицы C известно следующее:

1. $\det\ (C(1|1)) \neq 0$.

2. Вектор b_1 выражается не менее чем через $p-2$ строки матрицы $C(1|1)$, а значит среди чисел $\det\ (C(i|1))$, где $i = 2, \ldots, n$ не менее чем $p-2$ числа, отличных от 0.

Разложим определитель матрицы C по первому столбцу:

$$\det\ (C) = c_{11}\det\ (C(1|1)) - \ldots + (-1)^{n+1}c_{n1}\det\ (C(n|1))$$

Так как $c_{i1} \neq 0$, $i = \overline{1, \ldots, n}$, то в последнем равенстве не менее $(p-1)$ отличных от 0 слагаемых, а значит по лемме 3.2.26 можно так умножить некоторые из слагаемых на минус один, что будет получен любой элемент из F_p, в частности, число, равное перманенту исходной матрицы. Пусть эти множители образуют первый столбец матрицы U, остальные элементы которой равны единицам. Тогда будем иметь равенство $\mathrm{per}\ (A) = \det\ (C \circ U) = \det\ (A \circ X \circ U) = \det\ (A \circ Z)$. Построили матрицу $Z \in M_n(\pm 1)$, которая конвертирует матрицу A. Теорема доказана. $\square$

Замечание 3.2.30. Вполне неразложимость матрицы A является существенным условием в теореме 3.2.29. Действительно, пусть $p > 3$ и n достаточно большое, чтобы $n \geq (p-3)\log(n-1)(p-1)+2$. Возьмем в качестве матрицы A полученную из матрицы $J_3 \oplus I_{n-3}$ заменой всех элементов выше главной диагонали на единицы. Последовательно применяя формулу Лапласа разложения по последней строке к полученной матрице, получим, что $\mathrm{per}\,(A) = \mathrm{per}\,(J_3) = 6 \neq 0$, так как характеристика поля равна $p > 3$. Таким образом, выполнены все условия теоремы 3.2.29, кроме вполне неразложимости матрицы A. Построенная матрица A будет конвертируема тогда и только тогда, когда конвертируема матрица J_3. Из леммы 3.2.13 следует, что матрица J_3 неконвертируема для любого поля характеристики $p > 3$, а значит неконвертируема построенная матрица A.

Пример 3.2.31. Теорема 3.2.29 позволяет доказать конвертируемость некоторых матриц. Например, дана вполне неразложимая матрица $A \in M_{14}(\mathbb{F}_5)$, в которой существует строка и столбец без нулевых элементов. Так как $M = 2\log(13 \cdot 4) + 2 < 14$, то по теореме 3.2.29 матрица A конвертируема.

Следствие 3.2.32. Пусть $A \in M_n(\mathbb{F}_p)$ заполнена ненулевыми элементами, где $p > 2$ — простое число и n удовлетворяет неравенству

$$n \geq (p-3)\log(n-1)(p-1)+2.$$

Тогда матрица A конвертируема.

Доказательство. По определению матрица без нулевых элементов будет вполне неразложимой. Имеет место неравенство

$$n \geq (p-3)\log(n-1)(p-1)+2 > 2p-6.$$

Это означает, что выполнены все условия теоремы 3.2.29 и матрица A конвертируема. □

Следствие 3.2.33. Пусть $A \in M_n(\mathbb{F}_p)$ — частично разложимая матрица, перестановочно эквивалентная блочной верхнетреугольной матрице с вполне неразложимыми блоками $A_1, \ldots, A_k$ на главной диагонали, один из которых удовлетворяет условиям теоремы 3.2.29. Тогда матрица A конвертируема.

Доказательство. Без ограничения общности, можно считать, что блок A_1 удовлетворяет требованиям теоремы 3.2.29. Тогда, согласно доказательству теоремы 3.2.29, для любого $r \in \mathbb{F}_p$ существует матрица $X_r \in M_{k_1}(\pm 1)$ такая, что $\det\,(A_1 \circ X_r) = r$. Так как блоки A_i вполне неразложимы, то в каждом из них существует ненулевая обобщенная диагональ. По следствию 3.2.27 для каждого из блоков $A_2, \ldots, A_k$ существует матрица $Y_i \in M_{k_i}(\pm 1)$ такая, что $\det\,(A_i \circ Y_i) \neq 0$ при $i = 2, \ldots, k$. Остается заметить, что определитель

$$\det\,(A') = \det\,(A_1 \circ X_r) \prod_{i=2}^{k} \det\,(A_i \circ Y_i)$$

может принимать любое значение, так как первый сомножитель может принимать любое значение в поле, а остальные сомножители не равны нулю. Остается подобрать требуемое значение параметра r.

Если среди блоков есть нулевой, то в матрице не существует обобщенной диагонали без нулевых элементов, а значит $\mathrm{per}\,(A) = \det\,(A) = 0$. □

Рассмотрим еще одно достаточное условие конвертации матрицы над конечным полем с точки зрения существенных элементов.

Теорема 3.2.34. Пусть $A \in M_n(\mathbb{F}_p)$, где p — простое число. Пусть в какой-либо строке матрицы A содержится не менее $(p-1)$-го существенно ненулевых в смысле определителя элементов. Тогда матрица A конвертируема.

Доказательство. Без ограничения общности, можно считать, что в первой строке содержится не менее $(p-1)$ существенно ненулевых в смысле определителя элементов. Разложим определитель матрицы A по первой строке:

$$\det\,(A) = \sum_{i=1}^{n} (-1)^{i+1} a_{1i} \det\,(A(1|i)) \tag{3.13}$$

В сумме (3.13) не менее $(p-1)$-го ненулевого слагаемого. По следствию 3.2.22 в правой части (3.13) можно умножить часть слагаемых на минус один так, чтобы получить любой наперед заданное число из $\mathbb{F}_p$, в частности $P = \mathrm{per}\,(A)$. Рассмотрим теперь матрицу $X \in M_n(\pm 1)$, где минус единицы стоят только в первой строке на местах с теми номерами, для которых необходимо поменять знак в сумме (3.13). Получим равенство:

$$\det\,(A \circ X) = \sum_{i=1}^{n} (-1)^{i+1} x_{1i} a_{1i} \det\,(A(1|i) \circ X(1|i)) =$$

$$\sum_{i=1}^{n} (-1)^{i+1} x_{1i} a_{1i} \det\,(A(1|i)) = P = \mathrm{per}\,(A)$$

Построенная матрица X конвертирует матрицу A. □

Замечание 3.2.35. Требование существования $(p-1)$-го элемента существенно не равного нулю в смысле опеределителя вероятно является излишним и может быть заменено на существование $(p-1)$-го существенного элемента в одном строке (столбце) матрицы $A \in M_n(\mathbb{F}_p)$.

3.3 Тензор перманента и его свойства

Определение 3.3.1. Пусть $e_1, \ldots, e_n$ — стандартный базис линейного пространства $V_n = \mathbb{F}_q^n$. Пусть $A \in M_{k,n}(\mathbb{F}_q)$, где $k < n$. Рассмотрим $(n-k)$-мерный контравариантный тензор $T_A = T_A^{i_1,\ldots,i_{n-k}}$ заданный на пространстве $V_n^{n-k} = \underbrace{V_n \otimes \ldots \otimes V_n}_{n-k \text{ раз}}$. Зададим компоненты тензора в базисе $e_1, \ldots, e_n$ по правилу:

$$T_A^{i_1,\dots,i_{n-k}} = \begin{cases} \operatorname{per}\,(A(|i_1,\dots,i_{n-k})), \text{ если все } i_1,\dots,i_{n-k} \text{ различны} \\ 0 \text{ в противном случае.} \end{cases}$$

Тензор T_A будем называть тензором перманента матрицы A. В случае, если $k=1$, матрица может быть рассмотрена как вектор $A \in M_{1,n}(\mathbb{F}_q) = \mathbb{F}_q^n$, и мы будем называть T_A тензором вектора A.

Лемма 3.3.2. Пусть задан вектор $a \in \mathbb{F}_q^n$. Тогда $T_a \equiv 0$ тогда и только тогда, когда $a \equiv 0$.

Доказательство. Если $a = 0$, то легко видеть, что $T_a^{i_1,\dots,i_{n-1}} = 0$ для всех наборов $i_1,\dots,i_{n-1}$. Наоборот, если существует такой индекс i, $1 \le i \le n$, что $a_i \ne 0$, то для

$$\{i_1,\dots,i_{n-1}\} = \{1,\dots,i-1,i+1,\dots,n\}$$

имеем $T_a^{i_1,\dots,i_{n-1}} = a_i \ne 0$, а значит $T \not\equiv 0$. □

Лемма 3.3.3. Пусть заданы матрица $A \in M_{k,n}(\mathbb{F}_q)$ и тензор T_A. Тензор T_A симметричен, то есть для любого набора $i_1,\dots,i_{n-k}$ и любой перестановки $\sigma \in S_{n-k}$ имеет место равенство: $T_A^{i_1,\dots,i_{n-k}} = T_A^{i_{\sigma(1)},\dots,i_{\sigma(n-k)}}$.

Доказательство. Так как любая перестановка может быть представлена как произведение транспозиций, то достаточно доказать утверждение леммы для произвольной транспозиции.

Если среди $i_1,\dots,i_{n-k}$ есть одинаковые индексы, то по определению компонент тензора T_A имеем $T_A^{i_1,\dots,i_{n-k}} = 0$. После перестановки индексов среди них по-прежнему останутся одинаковые, а значит

$$T_A^{i_1,\dots,i_{n-k}} = 0 = T_A^{i_{\sigma(1)},\dots,i_{\sigma(n-k)}}.$$

Таким образом, можно считать, что $i_1, \ldots, i_{n-k}$ различны. Тогда $T_A^{i_1,\ldots,i_{n-k}} = \text{per}\ (A(|i_1, \ldots, i_{n-k}))$. Так как при любой перестановке вычеркиваемых столбцов выражение per $(A(|i_1, \ldots, i_{n-k}))$ не изменяется, то для любой перестановки $\sigma \in S_{n-k}$ имеем равенство

$$T_A^{i_1,\ldots,i_{n-k}} = \text{per}\ (A(|i_1, \ldots, i_{n-k})) =$$

$$\text{per}\ (A(|i_{\sigma(1)}, \ldots, i_{\sigma(n-k)})) = T_A^{i_{\sigma(1)},\ldots,i_{\sigma(n-k)}},$$

что и требовалось доказать. □

Определение 3.3.4. Пусть $a = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ — вектор с n компонентами. Пусть $A \in M_{k,n}(\mathbb{F}_q)$, T_A обозначает тензор перманента матрицы A. Сверткой тензора T_A и вектора a называется тензор $\overline{T} = T_A \circ a$, компоненты которого заданы по следующему правилу:

$$\overline{T}^{i_1,\ldots,i_{n-k-1}} = \sum_{j=1}^{n} T^{i_1,\ldots,i_{n-k-1},j} \cdot a_j.$$

Лемма 3.3.5. Пусть $B \in M_{(k+1),n}(\mathbb{F}_q)$, вектор a равен первой строке матрицы B и $A = B(1|) \in M_{k,n}(\mathbb{F}_q)$, где $k < n$. Тогда имеет место равенство:

$$T_B = T_A \circ a.$$

ДОКАЗАТЕЛЬСТВО. Докажем покомпонентное равенство T_B и $T_A \circ a$. По определению операции свертки имеем:

$$(T_A \circ a)^{i_1,\ldots,i_{n-k-1}} = \sum_{j=1}^{n} T_A^{i_1,\ldots,i_{n-k-1},j} \cdot a_j.$$

Если среди индексов $i_1, \ldots, i_{n-k-1}$ есть одинаковые, то по определению тензора перманента имеем равенства

$$T_B^{i_1,\ldots,i_{n-k-1}} = 0 \quad T_A^{i_1,\ldots,i_{n-k-1},j} = 0$$

для любого j, а значит $(T_A \circ a)^{i_1,\dots,i_{n-k-1}} = 0$, то есть равенство выполняется. Таким образом, далее можно считать, что все индексы $i_1, \dots, i_{n-k-1}$ различны. В силу определения тензора перманента, имеет смысл учитывать только те слагаемые, для которых все координаты $i_1, \dots, i_{n-k-1}, j$ различны, остальные слагаемые вносят нулевой вклад в сумму. Итого имеем:

$$(T_A \circ a)^{i_1,\dots,i_{n-k-1}} = \sum_{j=1}^{n} T_A^{i_1,\dots,i_{n-k-1},j} \cdot a_j =$$

$$= \sum_{j \in [1,n] \setminus [i_1,\dots,i_{n-k-1}]} \mathrm{per}\ (A(|i_1, \dots, i_{n-k-1}, j))a_j =$$

(с учетом того, что A — подматрица B, образованная всеми строками, кроме первой)

$$= \sum_{j \in [1,n] \setminus [i_1,\dots,i_{n-k-1}]} \mathrm{per}\ (B(1|i_1, \dots, i_{n-k-1}, j))a_j =$$

$$= \mathrm{per}\ (B(|i_1, \dots, i_{n-k-1})) = T_B^{i_1,\dots,i_{n-k-1}},$$

что и требовалось доказать. □

Теорема 3.3.6. Пусть матрица $A \in M_n(\mathbb{F}_q)$ представлена как набор строк $a_1, \dots, a_n$. Тогда для перманента матрицы A справедлива формула:

$$\mathrm{per}\ (A) = (...(T_{a_n} \circ a_{n-1}) \circ a_{n-2} \dots) \circ a_1.$$

Доказательство. Рассмотрим $T_{A(1,\dots,n-1|)} = T_{a_n}$. Последовательно применяя лемму 3.3.5 для свертки вида $T_{A(1,\dots,k|)} \circ a_k$, получим требуемое равенство:

$$T_{A(|)} = (...(T_{A(1,\dots,n-1|)} \circ a_{n-1}) \circ a_{n-2} \dots) \circ a_1. \tag{3.14}$$

□

3.4 Биективная конвертация

3.4.1 Оценка числа матриц с нулевым перманентом

Определение 3.4.1. Будем говорить, что биективное отображение

$$T : M_n(\mathbb{F}_q) \to M_n(\mathbb{F}_q)$$

осуществляет биективную конвертацию перманента в определитель, если для любой матрицы $A \in M_n(\mathbb{F}_q)$ выполнено равенство

$$\mathrm{per}\ (A) = \det\ (T(A)).$$

Обозначение 3.4.2. Пусть $M_n(\mathbb{F}_q)$ — множество квадратных матриц размера n над полем $\mathbb{F}_q$. Для подмножества $X \subset M_n(\mathbb{F}_q)$ введем следующие функции:

1. $P(X) = |\{A \in X : \mathrm{per}\ (A) = 0\}|$
2. $D(X) = |\{A \in X : \det\ (A) = 0\}|$

Замечание 3.4.3. Числа $P(M_n(\mathbb{F}_q))$ и $D(M_n(\mathbb{F}_q))$ равны мощности ядер функций перманента и определителя в пространстве матриц над конечным полем $\mathbb{F}_q$.

Лемма 3.4.4 (Артин, [1])**.** Имеет место следующая формула для числа элементов в ядре определителя матрицы из $M_n(\mathbb{F}_q)$:

$$D(M_n(\mathbb{F}_q)) = q^{n^2} - \prod_{k=1}^{n}(q^n - q^{k-1}).$$

Замечание 3.4.5. Вопрос явного вычисления функции $P(M_n(\mathbb{F}_q))$ на сегодняшний день является открытым (см., например, [17]).

Лемма 3.4.6. Пусть T_A — тензор перманента матрицы $A \in M_{k,n}(\mathbb{F}_q)$. Пусть тензор $T_A \not\equiv 0$, то есть содержит хотя бы одну ненулевую компоненту $T_A^{i_1,\dots,i_{n-k}}$. Тогда существует $q^k(q^{n-k}-1)$ различных векторов $a \in F_q^n$ таких, что $R = T_A \circ a \not\equiv 0$.

Доказательство.

1. Без ограничения общности можно считать, что $T_A^{1,\dots,n-k} \neq 0$.

2. Будем искать векторы a следующим образом: выберем произвольным образом последние k компонент вектора a (всего q^k способов) и покажем, что для каждого такого выбора существует не менее $q^{n-k}-1$ возможностей выбора остальных $n-k$ компонент, при котором значение R отлично от нуля, то есть при фиксированных последних k компонентах вектора, не более одного набора первых компонент дает нулевое значение тензора R. Для этого оценим сверху число способов выбрать $(n-k)$ оставшихся координат вектора a, чтобы выполнялось условие $R = 0$.

3. Равенство тензора R нулю означает, что $R^{j_1,\dots,j_{n-k-1}} = 0$ для любого набора $j_1,\dots,j_{n-k-1}$. Следовательно, в частности, имеют место равенства:

$$R^{1,\dots,n-k-1} = 0, R^{2,\dots,n-k} = 0, R^{3,\dots,n-k,1} = 0, \dots, R^{n-k,1,\dots,n-k-2} = 0,$$

где каждая следующая компонента получена циклическим сдвигом координат $1,\dots,n-k$ и зачеркиванием той, которая получилась последней.

4. Таким образом, получена система из $n-k$ уравнений на неизвестные координаты $a_1,\dots,a_{n-k}$:

$$\begin{cases} R^{1,\dots,n-k-1} = 0 \\ R^{2,\dots,n-k} = 0 \\ R^{l,\dots,n-k-1,1,\dots,l-2} = 0, \quad l = 3,\dots,n-k. \end{cases}$$

Последняя система является необходимым требованием для равенства $R = 0$, но, вообще говоря, не являются достаточным.

5. Перепишем последнюю систему, выражая компоненты тензора R через компоненты тензора T и вектора a по правилам свертки:

$$R^{1,\dots,n-k-1} = \sum_{j=1}^{n} T_A^{1,\dots,n-k-1,j} \cdot a_j; \qquad R^{2,\dots,n-k} = \sum_{j=1}^{n} T_A^{2,\dots,n-k,j} \cdot a_j;$$

$$R^{l,\dots,n-k-1,1,\dots,l-2} = \sum_{j=1}^{n} T_A^{l,\dots,n-k,1,\dots,l-2,j} \cdot a_j, \quad l = 3, \dots, n-k.$$

Тогда, учитывая, что компоненты тензора с двумя одинаковыми индексами равны нулю, имеем:

$$\begin{cases} T_A^{1,\dots,n-k} a_{n-k} + \sum\limits_{j=n-k+1}^{n} T_A^{1,\dots,n-k-1,j} a_j = 0 \\ T_A^{2,\dots,n-k,1} a_1 + \sum\limits_{j=n-k+1}^{n} T_A^{2,\dots,n-k,j} a_j = 0 \\ T_A^{l,\dots,n-k,1,\dots,l-1} a_{l-1} + \sum\limits_{j=n-k+1}^{n} T_A^{l,\dots,n-k,1,\dots,l-2,j} a_j = 0, \quad l = 3, \dots, n-k. \end{cases} \tag{3.15}$$

6. Компоненты $a_{n-k+1}, \dots, a_n$ вектора a фиксированы, значит $\sum\limits_{j=n-k+1}^{n} T_A^{1,\dots,n-k-1,j} a_j = C_1$, где $C_1 \in \mathbb{F}_q$ — некоторая константа, не зависящая от искомых величин $a_1, \dots, a_{n-k}$. Аналогично, $\sum\limits_{j=n-k+1}^{n} T_A^{l,\dots,n-k,1,\dots,l-2,j} a_j = C_l \in \mathbb{F}_q$ — константа для каждого $l = 2, \dots, n-k$.

7. Согласно лемме 3.3.3 тензор T симметричен, а значит имеет место равенство компонент:

$$T^{1,\dots,n-k} = T^{l,\dots,n-k,1,\dots,l-1} = D \ , \ l = 2, \dots, n-k,$$

где $D \in \mathbb{F}_q$ — константа, причем $D \neq 0$ согласно исходному предположению леммы.

8. Таким образом, перенося константы $C_i,\ i = 1, \dots, n-k$, в правую часть, систему (3.15) можно переписать в виде:

$$\begin{pmatrix} D & 0 & \dots & 0 \\ 0 & D & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & D \end{pmatrix} \begin{pmatrix} a_{n-k} \\ \dots \\ \dots \\ a_1 \end{pmatrix} = \begin{pmatrix} C_1 \\ \dots \\ \dots \\ C_{n-k} \end{pmatrix} \tag{3.16}$$

9. Так как D отлично от 0, система (3.16) имеет невырожденную матрицу коэффициентов, а значит имеет единственное решение.

10. Таким образом, мы получили, что для любого набора $a_{n-k+1}, \dots, a_n$ всего один набор координат $a_1, \dots, a_{n-k}$ удовлетворяет условию

$$R^{1,\dots,n-k-1} = \dots = R^{n-k,1,\dots,n-k-3} = 0,$$

которое является необходимым для тождества $R \equiv 0$.

11. Тогда существует не менее $q^k(q^{n-k} - 1)$ наборов таких, что $R \not\equiv 0$, что и требовалось доказать. ☐

Замечание 3.4.7. Обратим внимание, что в последней лемме не было найдено точное количество векторов a, а была доказана лишь нижняя оценка.

Лемма 3.4.8. Пусть T_a — тензор вектора $a = (1, \dots, 1) \in \mathbb{F}_q^n$, $n \geq 3$. Тогда количество векторов $b \in \mathbb{F}_q^n$ таких, что $R = T_a \circ b \neq 0$, равняется $q^n - 1$.

Доказательство. Докажем, что существует единственный способ выбрать вектор b такой, что $R = 0$. Для этого представим условие $R = 0$ в виде системы уравнений на неизвестные коэффициенты вектора b и определим число решений этой системы.

1. Начнем с рассмотрения условий $R^{1,\dots,n-2} = R^{1,\dots,n-3,n-1} = R^{1,\dots,n-3,n} = 0$. Это равносильно тому, что

$$\operatorname{per}\begin{pmatrix} b_{n-1} & b_n \\ 1 & 1 \end{pmatrix} = 0; \quad \operatorname{per}\begin{pmatrix} b_{n-2} & b_n \\ 1 & 1 \end{pmatrix} = 0; \quad \operatorname{per}\begin{pmatrix} b_{n-2} & b_{n-1} \\ 1 & 1 \end{pmatrix} = 0.$$

Получившуюся систему уравнений можно переписать в виде:

$$\begin{cases} b_{n-1} + b_n = 0 \\ b_{n-2} + b_n = 0 \\ b_{n-2} + b_{n-1} = 0. \end{cases}$$

Последняя система имеет единственное решение $b_{n-2} = b_{n-1} = b_n = 0$. Заметим, что именно здесь возникает различие между определетелем и перманентом, так как соответствующая система уравнений для определителя имела бы несколько решений.

2. Чтобы показать, что $b_k = 0$, $k = 1, \ldots, n-3$, рассмотрим равенства $R^{1,\ldots,k-1,k+1,\ldots,n-1} = 0$, которое должно выполняться в силу условия $R = 0$. Таким образом, получаем:

$$R^{1,\ldots,k-1,k+1,\ldots,n-1} = \operatorname{per} \begin{pmatrix} b_k & b_n \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} b_k & 0 \\ 1 & 1 \end{pmatrix} = b_k = 0, \text{ где } k = \overline{1, \ldots, n-3}.$$

Это означает, что существует единственный вектор $b = (0, \ldots, 0)$ такой, что $R = T_a \circ b = 0$, а значит существует $(q^n - 1)$ векторов b таких, что $R \neq 0$. □

Теорема 3.4.9. Пусть $\mathbb{F}_q$ — конечное поле из q элементов, характеристика которого больше 2. Тогда имеет место неравенство: $D(M_n(\mathbb{F}_q)) \geq P(M_n(\mathbb{F}_q))$.

Доказательство. Оценим снизу количество матриц с ненулевым перманентом. При фиксированном n будем доказывать индукцией по числу k строк длины n, что существует не менее

$$\prod_{j=1}^{k} (q^n - q^{j-1}) \tag{3.17}$$

матриц из $M_{k,n}(\mathbb{F}_q)$, тензор перманента которых ненулевой. Тогда при $n = k$ получим утверждение теоремы.

1. База индукции. Существует (q^n-1) способов выбрать ненулевую строку. По лемме 3.3.2 тензор перманента каждой из этих строк отличен от нуля.

2. Шаг индукции. Предположим, что для всех $k \times n$-матриц утверждение доказано. Тогда, согласно лемме 3.4.6, существует $q^k(q^{n-k}-1) = q^n - q^k$ способов дополнить каждую из имеющихся $\prod\limits_{j=1}^{k}(q^n - q^{j-1})$ матриц еще одной строкой так, чтобы тензор перманента получившейся матрицы был отличен от нуля, то есть всего существует $\prod\limits_{j=1}^{k}(q^n - q^{j-1})(q^n - q^k) = \prod\limits_{j=1}^{k+1}(q^n - q^{j-1})$, что доказывает формулу 3.17.

3. По теореме 3.3.6 при $k = n$ тензор перманента — это скаляр, равный перманенту полученной матрицы. Таким образом, построили не менее

$$\prod_{k=1}^{n}(q^n - q^{k-1})$$

различных матриц, с ненулевым перманентом. По лемме 3.4.4 получаем неравенство:

$$P(M_n) \leq q^{n^2}\prod_{k=1}^{n}(q^n - q^{k-1}) = D(M_n).$$

□

Теорема 3.4.10. Пусть $\mathbb{F}_q$ — конечное поле из q элементов, характеристика которого больше 2. Тогда имеет место неравенство:

$$D(M_n(\mathbb{F}_q)) > P(M_n(\mathbb{F}_q)).$$

Доказательство. Согласно лемме 3.4.8, если в предыдущем доказательстве в качестве первой строки строящейся матрицы выбрать вектор $a = (1, \ldots, 1)$, то существует $q^n - 1$ способ выбрать вторую строку так, что тензор перманента получившейся $2 \times n$ матрицы отличен от нуля. Таким образом, количество матриц с ненулевым перманентом оценивается снизу следующим выражением:

$$q^{n^2} - P(M_n) \geq (q^n - 2)\prod_{k=2}^{n}(q^n - q^{k-1}) + (q^n - 1)\prod_{k=3}^{n}(q^n - q^{k-1}) =$$

$$= ((q^n - 2)(q^n - q) + (q^n - 1))\prod_{k=3}^{n}(q^n - q^{k-1}) >$$

$$> (q^n - 1)(q^n - q)\prod_{k=3}^{n}(q^n - q^{k-1}) = q^{n^2} - D(M_n)$$

Здесь второе слагаемое отвечает тем матрицам с ненулевым перманентом, у которых первая строка есть вектор $a = (1, \ldots, 1)$, а первое слагаемое — всем остальным матрицам с ненулевым перманентом.

Таким образом, получаем строгое неравенство $D(M_n(\mathbb{F}_q)) > P(M_n(\mathbb{F}_q))$. □

Оценим разницу между числом матриц с нулевым перманентом и ненулевым определителем.

Теорема 3.4.11. Пусть $\mathbb{F}_q$ — конечное поле из q элементов, характеристика которого больше 2. Тогда

$$D(M_n(\mathbb{F}_q)) - P(M_n(\mathbb{F}_q)) \geq (q-1)\prod_{k=3}^{n}(q^n - q^{k-1}).$$

Доказательство. Из доказательства теоремы 3.4.10 следует, что

$$D(M_n(\mathbb{F}_q)) - P(M_n(\mathbb{F}_q)) \geq$$

$$\geq (q^n - 2)\prod_{k=2}^{n}(q^n - q^{k-1}) + (q^n - 1)\prod_{k=3}^{n}(q^n - q^{k-1}) - \prod_{k=1}^{n}(q^n - q^{k-1}) =$$

$$= (q-1)\prod_{k=3}^{n}(q^n - q^{k-1}).$$

□

3.4.2 Отсутствие биективного отображения, конвертирующего перманент в определитель

Теорема 3.4.12. Пусть $\mathbb{F}_q$ — конечное поле из q элементов, char $(\mathbb{F}_q) = p \geq 3$, $M_n(\mathbb{F}_q)$ — кольцо квадратных матриц, где $n \geq 3$. Тогда не существует биективного отображения

$$G : M_n(\mathbb{F}_q) \to M_n(\mathbb{F}_q),$$

такого, что per $(A) =$ det $(G(A))$.

Доказательство. Так как количество матриц в $M_n(\mathbb{F}_q)$ конечно, то необходимым условием существования G является равенство $D(M_n(\mathbb{F}_q)) = P(M_n(\mathbb{F}_q))$. По теореме 3.4.10 это равенство не достигается, а значит указанного G не существует. □

Замечание 3.4.13. Конкретные вычисления для перманента при $n = 3, 4$ и сравнение с ранее полученными оценками показывают, что полученные оценки:

1. Согласуются с оценками, полученными в работе [17].

2. Полученная оценка не обязательно является точной даже по порядку и может далее улучшаться.

Замечание 3.4.14. В теореме 3.2.11 было доказано, что любая матрица $A \in M_n(\mathbb{F}_3)$ конвертируема. Полученный в теореме 3.4.12 говорит о том, что не существует универсальной матрицы $X \in M_n(\pm 1)$, которая бы конвертировала любую матрицу $A \in M_n(\mathbb{F}_3)$.

Литература

[1] Э. Артин. *Геометрическая алгебра.* Мир, М., 1969.

[2] Ф.Р. Гантмахер. *Теория матриц.* Наука, М., 1968.

[3] А.Э. Гутерман. Тезисы доклада. $10^{ая}$ *Международная конференция по конечным полям и их приложениям*, Гент, Бельгия, 11-15 июля 2011.

[4] А. Гутерман, Г. Долинар, Б. Кузьма. Барьеры Гибсона для проблемы Полиа. *Фундамент. и прикл. матем.*, **16(8)**:73-76, 2010.

[5] А. Гутерман, Г. Долинар, Б. Кузьма. Проблема Полиа о конвертируемости для симметрических матриц. *Мат. заметки*, **92(5)**:684-698, 2012.

[6] Б. Кузьма. Об отображениях, сохраняющих иммананты. *Фундамент. и прикл. матем.*, **13(4)**:113-120, 2007.

[7] Х. Минк. *Перманенты.* Мир, М., 1982.

[8] В.Н. Сачков, В.Е. Тараканов. *Комбинаторика неотрицательных матриц.* Научное издательство “ТВП”, М., 2000.

[9] В.Е. Тараканов, Р.А. Заторский. О связи детерминантов с перманентами. *Мат. заметки*, **85(2)**:292-299, 2009.

[10] J.P.M. Binet. Mémoire sur un systéme de formules analytiques, et. leur application á des considérations géometriques. *J. Éc. Polyt.*, **9**:280-302, 1812.

[11] J. A. Bondy, U. S. R. Murty. *Graph Theory with Applications.* North-Holland, Amsterdam, 1981.

[12] R.A. Brualdi, H. Perfect. Extension of partial diagonals of matrices I. *Monatshefte Math.*, **75**:385-397, 1971.

[13] R.A. Brualdi, H.J. Ryser. *Combinatorial Matrix Theory.* Cambridge Univ. Press, 1991.

[14] R. A. Brualdi, B. L. Shader. On Sing-Nonsigular Matrices and the Conversion of the Permanent into the Determinant. *DIMACS Ser. in Discrete Math. and Theoret. Comput. Sci.*, **4**:117-134, 1991.

[15] R. A. Brualdi, B. L. Shader. *Matrices of sing-solvable linear systems.* Cambridge Univ. Press, 1995.

[16] A. L. Cauchy. Mémorire sur les fonctions qui ne peuvent obtenir que deux valeurs égales et de signes conraires par suite des transpositions opérées entre les variables qu'elles renferment. *J. de l'Éc. Polyt.*, **10**:29-119, 1812.

[17] G. Dolinar, A. Guterman, B. Kuzma, M. Orel. On the Pólya permanent problem over finite fields. *E. J. of Comb.*, **32**:116-132, 2011.

[18] G. Frobenius. Über matrizen aus nicht negativen elementen. *Sitzungsber. König. Preuss. Akad. Wiss.*, **26**:456-477, 1912.

[19] G. Frobenius. Über zerlegbare determinanten. *Sitzungsber. König. Preuss. Akad. Wiss.*, **XVIII**:247-277, 1917.

[20] J. von zur Gathen. Permanent and determinant. *Linear Algebra Appl.*, **96**:87-100, 1987.

[21] G. Hetyei. Rectangular configurations which can be covered by 2 × 1 rectangles. *Pécsi Tan. Foisk. Közl.*, **8**:351-367, 1964.

[22] P. M. Gibson. Conversion of the Permanent into the Determinant. *Proc.Amer.Math.Soc.*, **27**:471-476, 1976.

[23] K. Koh. Even circuits in directed graphs and Lovász' conjecture. *Bull. Malayasian Math. Soc.*, **7**:47-52, 1976.

[24] D. König. Line systems and determinants. *Math. Termész. Ért.*, **33**:221-229, 1915.

[25] D. König. Über graphen und ihre andwendung auf determinantentheorie und mengenlehre. *Math. Ann.*, **77**:453-465, 1916.

[26] C. H. C. Little. A characterization of convertible (0; 1)-matrices. *J. Combin. Theory Ser. B*, **18**:187-208, 1975.

[27] D.E. Littlewood. *The Theory of Group Characters and Matrix Representations of Groups (2nd ed.).* Oxford Univ. Press, 1950.

[28] D.E. Littlewood, A.R. Richardson. Group characters and algebras. *Phil. Trans. R. Soc. Lond. A*, **233**:99-141, 1934.

[29] L. Lovász, M. D. Plummer. *Matching Theory.* Elsevier, Amsterdam, 1986.

[30] M. Marcus, H. Minc. On the relation between the determinant and the permanent. *Illinois J. Math.*, **5**:376-381, 1961.

[31] W. McCuaig. Even dicycles. *J. Graph Theory*, **35**:46-68, 2000.

[32] W. McCuaig. Brace generation. *J. Graph Theory*, **38**:124-169, 2001.

[33] W. McCuaig. Pólya's permanent problem. *Elec. J. of Comb.*, **11**:1-83, 2004.

[34] T. Muir. On a class of symmetric permanent functions. *Proc. Roy. Soc. Edinburg*, **11**:409-418, 1882.

[35] M. D. Plummer. On n-extendable graphs. *Discrete Math.*, **31**:201-210, 1980.

[36] G. Pólya. Aufgabe 424. *Arch. Math. Phys.*, **20(3)**:271, 1913.

[37] N. Robertson, P. D. Seymour, R. Thomas. Permanents, Pfaffian orientations, and even derected circuits. *Anals of Mathematics*, **150**:925-975, 1999.

[38] P. D. Seymour. On the two-colouring of hypergraphs. *Quart. J. Math. Oxford*, **25**:303-312, 1974.

[39] G. Szegö. Lösungzu. *Arch. Math. Phys.*, **21**:291-292, 1913.

[40] C. Thomassen. Sign-nonsingular matrices and even cycles in directed graphs. *Linear Alg. Appls.*, **75**:27-41, 1986.

[41] C. Thomassen. The even cycle problem for planar directed graphs. *J. Algorithms*, **15**:61-75, 1993.

[42] M. F. Tinsley. Permanents of cyclic matrices. *Pacific J. Math.*, **10**:1067-1082, 1960.

[43] L. G. Valiant. The complexity of computing the permanent. *Theoret. Comput. Sci.*, **8**:189-201, 1979.

[44] V. V. Vazirani, M. Yannakakis. Pfaffian orientations, 0-1 permanents, and even cycles in directed graphs. *Discrete Appl. Math.*, **25**:179-190, 1989.

Публикации автора по теме диссертации

[1] М.В. Будревич. Арифметические матричные операции, сохраняющие конвертацию. *Записки научн. сем. ПОМИ*, **419**:26-42, 2013.

[2] М.В. Будревич. Построение неконвертируемых матриц. *Мат. заметки*, **96(2)**:186-193, 2014.

[3] M. Budrevich, A. Guterman. Permanent has less zeros than determinant over finite fields. *Contemporary Mathematics; Amer. Math. Soc.*, **579**:33-42, 2012. *А.Э. Гутерману принадлежат формулировки теорем 2.16, 2.17 и утверждения 2.5 - 2.10. М.В. Будревичу принадлежат доказательства теорем 2.14, 2.16, 2.17 и утверждений 2.11 и 2.12.*

[4] M.V. Budrevich, A.E. Guterman. On the Gibson bounds over finite fields. *Serdica Math.*, **38**:395-416, 2012. *М.В. Будревичу принадлежат главы 1 и 3, А.Э. Гутерману принадлежат главы 2 и 4.*

[5] М.В. Будревич. О проблеме Полиа конвертации перманента в определитель для пространства матриц над конечным полем. *Конференция "Ломоносов-2012". Тезисы докладов.*, Москва, 2012, электронное издание (http://lomonosov-msu.ru/archive/Lomonosov_2012/1795/43726_fe99.pdf).

[6] М.В. Будревич. Достаточное условие знаковой конвертируемости матрицы над конечным полем. *Конференция "Ломоносов-2014". Тезисы докладов.*, Москва, 2014, электронное издание (http://lomonosov-msu.ru/uploaded/2200/2200_43726_5166b6.pdf).

[7] M. Budrevich. Matrix convertibility over finite field. *7th Linear Algebra Workshop*, Ljubljana, Slovenia, 2014, электронное издание (http://www.law05.si/law14/abstracts/Budrevich.pdf).