Записки научных
семинаров ПОМИ
Том 463, 2017 г.

М. В. Будревич

КОЛИЧЕСТВО МАТРИЦ С НЕНУЛЕВЫМ ПЕРМАНЕНТОМ НАД КОНЕЧНЫМ ПОЛЕМ

§1. Введение

В работе исследуются классические функции перманента и определителя матрицы. Напомним их определения:

$$\operatorname{per} A = \sum_{\sigma \in S_n} a_{1\sigma(1)} \ldots a_{n\sigma(n)}; \quad \det A = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) a_{1\sigma(1)} \ldots a_{n\sigma(n)},$$

где S_n — группа перестановок на множестве из n элементов, а $\operatorname{sign}(\sigma)$ — знак перестановки $\sigma \in S_n$. Мы будем рассматривать множество матриц $M_{m,n}(\mathbb{F}_q)$ с m строками и n столбцами, $m \leqslant n$, над конечным полем $\mathbb{F}_q$ с q элементами характеристики p. Если $m = n$, то будем писать $M_{n,n} = M_n$. Через $V^n(\mathbb{F}_q)$ или просто V^n обозначим пространство векторов длинны n с элементами из $\mathbb{F}_q$. Для матрицы $A \in M_{m,n}$ через $A(\alpha|\beta)$, где $\alpha \subset \{1, \ldots, m\}$ и $\beta \subset \{1, \ldots, n\}$, обозначим матрицу, полученную из A вычеркиванием строк с номерами из α и столбцов с номерами из β.

Мы рассматриваем поля характеристики $p > 2$, так как при $p = 2$ имеется равенство $1 = -1$ и функции перманента и определителя совпадают как формальные выражения.

Перманент является удобной считающей функцией, к нахождению которой сводятся многие комбинаторные вопросы и задачи теории графов [1,11–13]. Основная трудность прикладного использования перманента заключается в сложности его вычисления. Хорошо известен алгоритм Райзера вычисления перманента [3] с асимптотической сложностью $O(n2^n)$. Более того, задача нахождения перманента даже для $(0,1)$-матрицы является $\#P$-сложной [10], что вычислительно эквивалентно проблеме Кука $P \neq NP$ [5,8,9]. В связи с этим большое количество работ посвящено исследованию матричных функций ϕ таких,

Ключевые слова: перманент, определитель, конвертация, конечные поля.
Работа автора поддержана грантом РНФ 17-11-01124.

что для множества всех матриц или для какого-то его подмножества выполняется равенство:

$$\operatorname{per} A = \det \phi(A). \tag{1.1}$$

В работе [6] было рассмотрено биективное отображение ϕ для множества $M_n(\mathbb{F}_q)$. Авторы показали, что при условии $p > 2$ и достаточно большом количестве элементов в поле (в зависимости от порядка матриц) количество матриц с нулевым перманентом меньше количества матриц с нулевым определителем. Данный результат улучшен в работе [4], где было доказано, что при $n \geqslant 3$ и для полей характеристики $p \geqslant 3$ количество матриц из $M_n(\mathbb{F}_q)$ с нулевым перманентом строго меньше количества матриц с нулевым определителем. В частности, при n, $p \geqslant 3$ не существует биективного отображения $\phi : \mathrm{M_n}(\mathbb{F}_\mathrm{q}) \to \mathrm{M_n}(\mathbb{F}_\mathrm{q})$, такого что для любой матрицы $A \in M_n(\mathbb{F}_q)$ выполнено (1.1). В [2] улучшена оценка на количество матриц $A \in M_n(\mathbb{F}_q)$ с нулевым перманентом.

Позднее в работе [7] приведено доказательство невозможности построения линейного отображения для матриц порядка n при условии, что $p \geqslant 3$ и в поле не менее n элементов.

Цель настоящей работы — получить улучшение нижней оценки на количество матриц $A \in M_n(\mathbb{F}_q)$ с ненулевым перманентом. Для этого вводится понятие p-зависимости на k векторах длинны n, где $n > k$. Оказывается, что при маленьких значениях k из p-зависимости векторов следует, что в векторах не может быть большого количества ненулевых элементов. Это свойство позволяет улучшить оценку, полученную в работах [2, 4].

В §2 вводится понятие p-зависимости и исследуется его связь с тензором перманента. В §3 доказывается, что при $n \geqslant 5$ к двум p-независимым векторам u, v нельзя добавить вектор w без нулевых элементов так, чтобы векторы u, v, w оказались p-зависимыми. В §4 полученный результат использован для улучшения оценки числа матриц с ненулевым перманентом.

§2. p-ЗАВИСИМОСТЬ

В этом параграфе мы введем понятие p-зависимости и покажем, как оно связано с тензором перманента. Напомним определение тензора перманента согласно работе [4].

Определение 2.1. Тензором перманента матрицы $A \in M_{m,n}(\mathbb{F})$, где $m \leqslant n$, называется тензор $T(A)$, компоненты которого определены следующим образом:

$$T_{i_1,\dots,i_{n-m}}=\begin{cases}\text{per } A(|i_1,\dots,i_m), \text{если индексы } i_1,\dots,i_{n-m} \text{различны;}\\ 0, \quad \text{если среди индексов } i_1,\dots,i_{n-m} \text{ есть одинаковые.}\end{cases}$$

Замечание 2.2. Мы будем говорить, что тензор T нулевой и писать $T = 0$, если все компоненты тензора равны нулю.

Замечание 2.3. Компоненты тензора перманента матрицы $A \in M_{m,n}$, где $m < n$, – это либо нули, либо перманенты квадратных подматриц порядка m. Таким образом, $T(A) = 0$ тогда и только тогда, когда перманент любой квадратной подматрицы порядка m матрицы A равен 0.

Определение 2.4. Векторы $v_1,\dots,v_k \in V^n(\mathbb{F}_q)$, где $k \leqslant n$, называются p-зависимыми, если перманент любой подматрицы порядка k матрицы $A \in M_{k,n}(\mathbb{F}_q)$, образованной этими векторами, равен 0.

Замечание 2.5. В случае замены функции перманента на функцию определителя p-зависимость превращается в обычную линейную зависимость векторов.

Следующее свойство p-зависимости следует из определений 2.1 и 2.4.

Лемма 2.6. *Пусть $v_1,\dots,v_k \in V^n(\mathbb{F}_q)$, $k \leqslant n$ и строки матрицы $A \in M_{k,n}(\mathbb{F}_q)$ образованы векторами $v_1,\dots,v_k$. Векторы $v_1,\dots,v_k$ p-зависимы тогда и только тогда, когда $T(A) = 0$.*

Далее докажем некоторые свойства p-зависимости, которые естественным образом переносятся с линейной зависимости векторов.

Лемма 2.7. *Пусть векторы $v_1,\dots,v_k \in V^n(\mathbb{F}_q)$ p-зависимы, $k < n$, $w \in V^n(\mathbb{F}_q)$. Тогда векторы $v_1,\dots,v_k, w$ являются p-зависимыми.*

Доказательство. Пусть матрица $A \in M_{k,n}$ образована векторами $v_1, v_2,\dots,v_k$ и матрица B получена из A приписыванием первой строки, равной w. По условию $T(A) = 0$. Выберем в B подматрицу C порядка $k+1$. Для нахождения per C применим формулу разложения перманента по первой строке:

$$\text{per } C = \sum_{i=1}^{k+1} c_{1i} \text{per } C(1|i).$$

Так как матрица $C(1|)$ по построению является подматрицей A, а $C(1|i)$ – квадратная матрица порядка k, то per $C(1|i)$ является элементом тензора $T(A) = 0$. Следовательно, per $C(1|i) = 0$ для любого $i \in \{1, \ldots, k+1\}$ и per $C = 0$. Так как это верно для любой подматрицы C порядка $k+1$ матрицы B, то $T(B) = 0$, и векторы $w, v_1, \ldots, v_k$ p-зависимы. $\square$

Следствие 2.8. *Пусть векторы $v_1, \ldots, v_k \in V^n(\mathbb{F}_q)$, $k \leqslant n$, и среди них есть $l < k$ p-зависимых векторов. Тогда векторы $v_1, \ldots, v_k$ p-зависимы.*

Замечание 2.9. В условиях следствия 2.8 при $k = n$ получаем, что если в квадратной матрице A порядка n существует $k < n$ p-зависимых строк (столбцов), то per $A = 0$.

§3. Еще одно свойство p-зависимости

Оказывается, что при небольшом количестве векторов p-зависимость накладывает существенное ограничение на количество ненулевых элеметов векторов. Рассмотрим требование p-зависимости в виде системы линейных уравнений, где роль неизвестных играют элементы тензора перманента. Для получения оценки требуется невырожденность матрицы, поэтому возникает дополнительное ограничение на характеристику поля. Следующая лемма наглядно демонстрирует данную закономерность.

Лемма 3.1. *Пусть $A \in M_{2,5}(\mathbb{F}_q)$, характеристика поля $p > 3$ и $T(A) \neq 0$. Пусть $w \in V^5(\mathbb{F}_q)$ состоит из ненулевых элементов и матрица B получена из A приписыванием строки w. Тогда $T(B) \neq 0$.*

Доказательство. Умножим столбцы матрицы B на элементы поля $\mathbb{F}_q$ так, чтобы все элементы первой строки, полученной приписыванием w, были равны 1. Это можно сделать, так как у вектора w нет нулевых компонент. Полученную матрицу обозначим B'. По построению $B'(1|) = A'$. При каждом таком умножении столбца матрицы B на ненулевую константу элементы тензоров $T(A)$ и $T(B)$ либо не изменяются, либо умножаются на соответствующую константу. Таким образом, $T(B') = 0$ тогда и только тогда, когда $T(B) = 0$, и $T(A') = 0$ тогда и только тогда, когда $T(A) = 0$.

Далее, без ограничения общности, положим $w = (1, 1, 1, 1, 1)$.

Представим требование $T(B)=0$ как систему линейных уравнений, построенную следующим образом.

1. Неизвестными являются компоненты тензора $T(A)$, определенные как перманенты подматриц порядка 2 (определение 2.1). Каждую такую подматрицу можно задать вектором длины 5 из двух 1 и трех 0, где единицы соответствуют номерам выбранных в матрице A столбцов. На векторах такого вида естественным образом задается лексикографический порядок; пронумеруем наши неизвестные согласно этому порядку. Всего таких неизвестных $C_5^2=10$.

2. Уравнения определяются требованием, что перманент каждой подматрицы порядка 3 матрицы B должен быть равен 0. Так как элементы первой строки матрицы B равны 1, то каждое уравнение, полученное разложением перманента по первой строке, является суммой трех неизвестных с коэффициентами 1. Всего имеем $C_5^3=10$ уравнений.

Таким образом, получили однородную систему линейных уравнений с матрицей D, где

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

В явном виде находим $\det D=-2^43$. Так как характеристика поля $p>3$, то $\det D\neq 0$, а значит, у соответствующей однородной системы линейных уравнений существует только нулевое решение. Элементы этого решения совпадают с нетривиальными компонентами тензора $T(A)$, который по предположению леммы не равен 0. Из полученного противоречия следует, что $T(B)\neq 0$. $\square$

Замечание 3.2. Аргументы леммы 3.1 можно повторить для $A\in M_{3,7}(\mathbb{F}_q)$, где $\mathbb{F}_q$ – поле характеристики $p>3$. В этом случае будет $C_7^3=C_7^4=35$ уравнений и неизвестных, а определитель полученной матрицы будет равен $-2^{15}3^6\neq 0$.

§4. Улучшение оценки

Применим результат леммы 3.1 для оценки снизу количества матриц $A \in M_{3,n}(\mathbb{F}_q)$, таких что $T(A) \neq 0$.

Обозначение 4.1. Через $P^+_{(k\times n)}$ обозначим количество $k \times n$ матриц $A \in M_n(\mathbb{F}_q)$ с ненулевым тензором перманента.

В работе [2] было найдено точное значение $P^+_{(2\times n)}$.

Лемма 4.2 ([2, лемма 2]). *Пусть $A \in M_{2,n}(\mathbb{F}_q)$, $\mathbb{F}_q$ – поле характеристики $p > 2$. Тогда*

$$P^+_{(k\times n)} = (q^n - 1)^2 - (q-1)^2(n + C_n^2(q-1)).$$

В доказательстве последней леммы содержится следующее вспомогательное утверждение.

Лемма 4.3 ([2, лемма 2, доказательство]). *Пусть $A \in M_{2,3}(\mathbb{F}_q)$, $\mathbb{F}_q$ – поле характеристики $p > 2$. Пусть в матрице A нет нулевой строки или нулевого столбца. Тогда $T(A) \neq 0$.*

Лемма 4.4. *Пусть $A \in M_{2,n}(\mathbb{F}_q)$, где $n \geqslant 7$, и $\mathbb{F}_q$ — поле характеристики $p > 3$. Пусть матрица A не содержит нулевых строк и нулевых столбцов. Пусть $w \in V^n(\mathbb{F}_q)$, $w \neq 0$ и матрица B получена из матрицы A присоединением строки w. Тогда выполняется одно из следующих условий*:

(1) *В одной из строк матрицы A не более двух ненулевых элементов. Тогда существует $q-1$ различных векторов w, таких что $T(B) = 0$.*
(2) *$T(B) \neq 0$.*

Доказательство. Пусть l_0 и l_+ – количества нулевых и ненулевых элементов в векторе w, $l_0 + l_+ = n$.

Если $l_+ \geqslant 5$, то мы можем выбрать 3×5 подматрицу C матрицы B, в первой строке которой нет нулей. Матрица $C(1|)$ является подматрицей A, и по условию в ней нет нулевых столбцов. Однако, так как это подматрица матрицы A, то в ней могут быть нулевые строки. Рассмотрим три варианта в зависимости от количества нулевых строк в матрице $C(1|)$.

1. Предположим, что в $C(1|)$ нет нулевых строк. Тогда в ней можно выбрать 2×3 подматрицу $C(1|i, j)$ без нулевых строк и столбцов. По лемме 4.3 получаем $T(C(1|i,j)) \neq 0$ и, следовательно, $T(C(1|)) \neq 0$. По лемме 3.1 $T(C) \neq 0$. Так как C – подматрица матрицы B с максимально возможным количеством строк, то элементы тензора $T(C)$ являются элементами тензора $T(B)$. Следовательно, $T(B) \neq 0$.

2. Предположим, что в матрице $C(1|)$ одна нулевая строка. Без ограничения общности можно считать, что это первая строка $C(1|)$. Так как столбцы $C(1|)$ являются столбцами A и не могут быть нулевыми, то во второй строке $C(1|)$ все элементы ненулевые. Таким образом, в матрице $C(2|)$ нет нулевых элементов. Выберем 2×3 подматрицу $C(2|i,j)$. В $C(2|i,j)$ нет нулевых элементов; следовательно, по лемме 4.3 $T(C(2|i,j)) \neq 0$. Выберем ненулевой элемент этого тензора; ему соответствует такая 2×2 подматрица $D = (d_{kl})$, что $\operatorname{per} D \neq 0$. Зафиксируем эти два столбца и еще один столбец матрицы B, второй элемент которого равен $a \neq 0$. Тогда они образуют подматрицу

$$\begin{pmatrix} d_{11} & d_{12} & * \\ 0 & 0 & a \\ d_{21} & d_{22} & * \end{pmatrix}.$$

Перманент последней матрицы равен $a\operatorname{per} D \neq 0$ и является элементом тензора $T(B)$. Следовательно, $T(B) \neq 0$.

3. Предположим, что в матрице $C(1|)$ две нулевые строки, то есть $C(1|) = 0$. Матрица $C(1|)$ является подматрицей матрицы A с максимальным количеством строк, следовательно, нулевые столбцы матрицы $C(1|)$ являются нулевыми столбцами матрицы A. Это противоречит условию леммы, а значит, такой вариант невозможен.

Далее рассмотрим $l_+ \leqslant 4$. Так как $n \geqslant 7$, то $l_0 \geqslant 3$. Заметим, что по условию $w \neq 0$ и $l_+ \geqslant 1$.

Выберем максимальную подматрицу C матрицы B, элементы первой строки которой равны 0. Количество столбцов этой матрицы равно $l_0 \geqslant 3$. Рассмотрим несколько вариантов в зависимости от количества нулевых строк в матрице $C(1|)$.

1. Предположим, что в $C(1|)$ нет нулевых строк. Тогда в ней найдется 2×3 подматрица без нулевых строк и столбцов, в которой по лемме 4.3 найдется такая 2×2 подматрица $D = (d_{ij})$, что $\operatorname{per} D \neq 0$. Матрица D является подматрицей $C(1|)$. Выберем в матрице B столбец, не вошедший в C. По построению, первый элемент этого столбца равен $a \neq 1$. Таким образом, в матрице B есть такая подматрица:

$$\begin{pmatrix} 0 & 0 & 1 \\ d_{11} & d_{12} & * \\ d_{21} & d_{22} & * \end{pmatrix}.$$

Перманент последней матрицы равен $\operatorname{per} D \neq 0$ и является элементом тензора $T(B)$. Следовательно, $T(B) \neq 0$.

2. Предположим, что в $C(1|)$ есть нулевая строка. Без ограничения общности можно считать, что это вторая строка матрицы C. Так как в $C(1|)$ нет нулевых столбцов, то третья строка матрицы C не содержит нулей. Пусть D дополняет матрицу C до матрицы B. Первая строка D содержит все ненулевые элементы первой строки B и не содержит нулевых элементов. Таким образом, в D в точности l_+ столбцов. Так как вторая строка C содержит только нулевые элементы, то вторая строка D содержит все ненулевые элементы второй строки B. Далее, в зависимости от количества ненулевых элементов в первой строке B, получаем следующие варианты:

2.1. Пусть $l_+ \geqslant 3$. Тогда в $D(3|)$ можно выбрать 2×3 подматрицу без нулевых строк и нулевых столбцов; по лемме 4.3, тензор этой подматрицы не равен 0. Следовательно, в $D(3|)$ существует 2×2 подматрица $F = (f_{ij})$, такая что $\operatorname{per} F \neq 0$. Возьмем столбцы, содержащие подматрицу F, и любой столбец матрицы C. По построению последний элемент столбца из матрицы C равен $a \neq 0$. Получили подматрицу матрицы B следующего вида:

$$\begin{pmatrix} 0 & f_{11} & f_{12} \\ 0 & f_{21} & f_{22} \\ a & * & * \end{pmatrix}.$$

Перманент последней матрицы равен $a \operatorname{per} F \neq 0$ и является элементом тензора $T(B)$, следовательно, $T(B) \neq 0$.

2.2. Пусть $l_+ = 2$. С точностью до перестановки столбцов матрица B имеет вид

$$\begin{pmatrix} 0 & 0 & \dots & 0 & w_1 & w_2 \\ 0 & 0 & \dots & 0 & b_{2,n-1} & b_{2n} \\ b_{31} & b_{32} & \dots & b_{3,n-2} & b_{3,n-1} & b_{3n} \end{pmatrix}.$$

Обозначим $F = \begin{pmatrix} w_1 & w_2 \\ b_{2,n-1} & b_{2n} \end{pmatrix}$. Если per $F = 0$, то первая и вторая строка B p-зависимы, а тогда, по лемме 2.7, строки B будут p-зависимыми; следовательно, $T(B) = 0$. Далее, рассмотрим подматрицу матрицы B, состоящую из трех последних столбцов. Если per $F \neq 0$, то перманент этой подматрицы равен $b_{3,n-2}$per $F \neq 0$ и $T(B) \neq 0$. Таким образом, $T(B) = 0$ тогда и только тогда, когда per $F = 0$.

Вычисляя перманент F находим per $F = w_1 b_{2n} + w_2 b_{2,n-1}$. Если $b_{2,n-1} = 0$ или $b_{2n} = 0$, то per $F \neq 0$ и $T(B) \neq 0$. Если $b_{2,n-1} \neq 0$ и $b_{2n} \neq 0$, то из равенства per $F = 0$ следует $w_1 = \frac{-w_2 b_{2,n-1}}{b_{2n}}$. Таким образом, для любого $w_2 \in \mathbb{F}_q$ такого, что $w_2 \neq 0$, существует единственный элемент w_1 такой, что выполнено равенство $T(B) = 0$. Всего существует $q-1$ способов выбрать $w_2 \neq 0$.

2.3. Пусть $l_+ = 1$. Тогда матрица B имеет вид

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 0 & w_1 \\ 0 & 0 & \dots & 0 & 0 & b_{2n} \\ b_{31} & b_{32} & \dots & b_{3,n-2} & b_{3,n-1} & b_{3n} \end{pmatrix}.$$

Так как первая и вторая строки матрицы B p-зависимы, то, по лемме 2.7, все строки матрицы B p-зависимы и $T(B) = 0$. При этом элемент $w_1 \in \mathbb{F}_q$, не равный 0, может быть выбран $q-1$ различными способами, а значит, существует $q-1$ различных векторов w таких, что $T(B) = 0$.

3. Предположим, что в $C(1|)$ две нулевые строки. Следовательно, $C(1|) = 0$, а так как столбцы $C(1|)$ являются столбцами матрицы A, то это противоречит условию, и такой случай невозможен. Лемма доказана. □

Далее мы построим оценку снизу на $P^+_{(3\times n)}$. Для этого нам понадобиться следующая лемма.

Лемма 4.5 ([4, лемма 2.11]). *Пусть $A \in M_{k,n}(\mathbb{F}_q)$, $\mathbb{F}_q$ – поле характеристики $p>2$ и $T(A) \neq 0$. Тогда существует не менее $q^k(q^{n-k}-1)$ векторов $w \in V^n(\mathbb{F}_q)$ таких, что для матрицы B, полученной объединением вектора w и матрицы A, имеет место неравенство $T(B) \neq 0$.*

Теорема 4.6. *Пусть $A \in M_{3,n}(\mathbb{F}_q)$, $\mathbb{F}_q$ – поле характеристики $p > 3$. Тогда*

$$P^+_{(3\times n)} \geqslant (q^n-1)((q^n-1)^2 - n(q-1) - 3C_n^2(q-1)(q+1)^2) - P^+_{(2\times 6)} C_n^6 (q^2-1).$$

Доказательство. Любая матрица $A \in M_{3,n}(\mathbb{F}_q)$ такая, что $T(A) \neq 0$, может быть представлена как объединение матрицы $B \in M_{2,n}(\mathbb{F}_q)$ с $T(B) \neq 0$ и вектора $w \in V^n$. Разобьем множество $2 \times n$ матриц с ненулевым тензором перманента на три подмножества в зависимости от того, как может быть к этим матрицам применена лемма 4.4.

1. Пусть в матрице $B \in M_{2,n}$ не более 6 ненулевых столбцов. Тогда мы не можем в ней выбрать подматрицу, к которой применима лемма 4.4. Всего таких матриц не более $C_n^6 P^+_{(2\times 6)}$. Для каждой такой матрицы по лемме 4.5 существует не менее $q^2(q^{n-2}-1)$ векторов w, которые позволяют построить матрицу A с $T(A) \neq 0$.

2. Пусть в матрице $B \in M_{2,n}$ есть строка с одним или двумя ненулевыми элементами. Всего таких матриц не более $2(q^n-1)C_n^2(q^2-1)$, где 2 отвечает за выбор строки с одним или двумя ненулевыми элементами, $q^n - 1$ – это число способов выбрать элементы строки, для которой не известно количество ненулевых элементов, C_n^2 – это число способов выбрать две позиции в строке, где количество ненулевых элементов ограничено двумя, и $q^2 - 1$ – число способов расположить ненулевые элементы на зафиксированных местах. Для каждой такой матрицы B, по лемме 4.4, существует в точности $q^n - q + 1$ векторов w, при которых $T(A) \neq 0$.

3. По лемме 4.4 для каждой матрицы $B \in M_{2,n}$, не вошедшей ни в первую, ни во вторую группы, существует $q^n - 1$ векторов w таких, что $T(A) \neq 0$.

Объединим эти оценки:

$$\begin{aligned} P^+_{(3\times n)} &\geqslant (P^+_{(2\times n)} - C_n^6 P^+_{(2\times 6)} - 2(q^n-1)C_n^2(q^2-1))(q^n-1) \\ &+ C_n^6 P^+_{(2\times 6)} q^2(q^{n-2}-1) + 2(q^n-1)C_n^2(q^2-1)(q^n-q+1). \end{aligned}$$

Перегруппируем слагаемые в зависимости от применимости леммы 4.4:

$$= P^+_{(2\times n)}(q^n-1) - P^+_{(2\times 6)} C_n^6(q^2-1) - 2C_n^2(q^n-1)(q^2-1)(q-2).$$

Подставим значение $P^+_{(2\times n)}$ и вынесем $(q^n - 1)$ из первого и третьего слагаемых:

$$(q^n-1)((q^n-1)^2-(q-1)^2(n+C_n^2(q-1))-2C_n^2(q^2-1)(q-2))-P^+_{(2\times 6)}C_n^6(q^2-1).$$

Перегруппируем слагаемые и вынесем C_n^2:

$$(q^n-1)((q^n-1)^2-n(q-1)^2-3C_n^2(q-1)(q+1)^2)-P^+_{(2\times 6)}C_n^6(q^2-1). \ \square$$

Замечание 4.7. Два старших члена в получившейся оценке – это $q^{3n}-3q^{2n}$. Комбинация оценок из работ [2,4] дает два старших члена $q^{3n}-q^{2n+2}$.

Следствие 4.8. *Пусть $\mathbb{F}_q$ – поле характеристики $p>3$. Тогда существует не менее*

$$((q^n-1)((q^n-1)^2-n(q-1)-3C_n^2(q-1)(q+1)^2) \\ -P^+_{(2\times 6)}C_n^6(q^2-1))\prod_{i=4}^{n} q^{i-1}(q^{n-i+1}-1)$$

матриц $A\in M_n(\mathbb{F}_q)$ таких, что $T(A)\neq 0$.

Доказательство. По теореме 4.6, существует не менее

$$(q^n-1)((q^n-1)^2-n(q-1)-3C_n^2(q-1)(q+1)^2)-P^+_{(2\times 6)}C_n^6(q^2-1)$$

матриц $A\in M_{3,n}(\mathbb{F}_q)$ таких, что $T(A)\neq 0$. Для каждой такой матрицы применим лемму 4.5 $n-3$ раза. $\square$

Замечание 4.9. Начиная с некоторого n, зависящего от q, оценка теоремы 4.6 лучше оценки, полученной в [2]. В таблице приведены минимальные значения парамента n в зависимости от q при которых новая оценка лучше старой:

q	5	7	11	13	17	19	23	25	29
n	31	27	21	20	18	17	16	16	15

Литература

1. В. Н. Сачков, В. Е. Тараканов, *Комбинаторика неотрицательных матриц.* Научное издательство ТПВ, М., 2000.
2. L. A. Bassalygo, *On the number of nonzero permanents over a finite field of odd characteristic.* — Probl. Inform. Transm. **49** (4) (2013), 382–83.
3. R. A. Brualdi, H. J. Ryser, *Combinatorial Matrix Theory.* Cambridge Univ. Press, 1991.
4. M. V. Budrevich, A. E. Guterman, *Permanent has less zeros than determinant over finite fields.* — Contemp. Math. **579** (2012), 33–42.
5. S. A. Cook, *The complexity of theorem proving procedures.* — Proc. 3rd Ann. ACM Symp. Theory of Computing (1971), 151–158.
6. G. Dolinar, A. Guterman, B. Kuzma, M. Orel, *On the Pólya permanent problem over finite fields.* — Eur. J. Comb. **32** (2011), 116–132.

7. M. A. Duffner, H. F. da Cruz, *A relation between the determinant and the permanent on singular matrices.* — Linear Algebra Appl. **438** (2013), 3654–3660.
8. M. R. Garey, D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completness*, W. H. Freeman, San Francisco, 1979.
9. R. M. Karp, *Reducibility among combinatorial problems.* — In: Complexity of Computer Computations, Plenum Press, New-York (1972), 85–104.
10. L. G. Valiant, *The complexity of computing the permanent.* — Theor. Comput. Sci. **8** (1979), 189–201.
11. W. McCuaig, *Pólya's permanent problem.* — Electron. J. Combin. **11** (2004), Research Paper 79.
12. H. Minc, *Permanents*, Addison-Wesley Publishing Company, Inc, 1978.
13. V. V. Vazirani, M. Yannakakis, *Pfaffian orientations,* 0-1 *permanents, and even cycles in directed graphs.* — Discrete Appl. Math. **25** (1989), 179–190.

Budrevich M. V. The number of matrices with nonzero permanent over a finite field.

A new method for obtaining lower bounds on the number of matrices over a finite field with nonzero permanent is developed. Some earlier results are improved.

Московский государственный университет
им. М. В. Ломоносова,
Ленинские горы, д. 1, Москва, Россия, 119991, ГСП-1
E-mail: MBudrevich@yandex.ru

Поступило 1 ноября 2017 г.